WAH7130

LTE Portable Router

Version 1.00
Edition 1, 03/2013

User's Guide

Default Login Details	
LAN IP Address	http://192.168.1.1
Password	1234

Copyright © 2013 ZyXEL Communications Corporation

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

  The Quick Start Guide shows how to connect the WAH7130 and access the Web Configurator. It contains information on setting up your network and configuring for Internet access.

Contents Overview

User's Guide 9

Introduction 11
Introducing the Web Configurator 17

Technical Reference 25

Monitor 27
WAN 33
Wireless LAN 41
LAN 49
DHCP Server 51
NAT 55
Firewall 63
Maintenance 69
Troubleshooting 77

Table of Contents

Contents Overview **3**

Table of Contents **5**

Part I: User's Guide **9**

Chapter 1
Introduction **11**

1.1 Overview 11
1.2 Ways to Manage the WAH7130 11
1.3 Good Habits for Managing the WAH7130 11
1.4 Hardware Installation 12
1.5 Resetting the WAH7130 12
1.5.1 How to Use the RESET Button 12
1.6 The Power/WPS Switch 13
1.6.1 Turn on/off the WAH7130 13
1.6.2 Enter Sleep/Normal Mode 13
1.6.3 Enable the OLED Display 14
1.6.4 Enable WPS 14
1.7 LED 15
1.8 OLED Icons 15

Chapter 2
Introducing the Web Configurator **17**

2.1 Overview 17
2.2 Accessing the Web Configurator 17
2.2.1 Login Screen 17
2.2.2 Password Screen 19
2.2.3 APN Screen 19
2.3 Status Screen 20
2.3.1 Navigation Panel 23

Part II: Technical Reference **25**

Chapter 3
Monitor **27**

3.1 Overview 27
3.2 What You Can Do 27
3.3 The Log Screen 27
3.3.1 View Log 27
3.4 DHCP Table 28
3.5 Packet Statistics 29
3.6 WLAN Station Status 30
3.7 Short Message Service (SMS) 31

Chapter 4
WAN 33

4.1 Overview 33
4.2 What You Can Do 33
4.3 What You Need To Know 33
4.4 Broadband Screen 35
4.5 Data Plan Screen 36
4.6 PIN Setting Screen 37
4.7 Change PIN Screen 39

Chapter 5
Wireless LAN....41

5.1 Overview 41
5.1.1 What You Can Do 42
5.1.2 What You Should Know 42
5.2 General Wireless LAN Screen 43
5.3 Guest Wi-Fi Screen 45
5.4 MAC Filter Screen 46

Chapter 6
LAN 49

6.1 Overview 49
6.2 What You Can Do 49
6.3 LAN IP Screen 49

Chapter 7
DHCP Server 51

7.1 Overview 51
7.1.1 What You Can Do 51
7.1.2 What You Need To Know 51
7.2 DHCP Server General Screen 51
7.3 DHCP Client List Screen 52

Chapter 8
NAT....55

8.1 Overview 55
8.1.1 What You Can Do 55
8.1.2 What You Need To Know 56
8.2 General 57
8.3 Port Forwarding Screen 57
8.3.1 Port Forwarding Edit Screen 59
8.4 Technical Reference 60
8.4.1 NAT Port Forwarding: Services and Port Numbers 60
8.4.2 NAT Port Forwarding Example 60

Chapter 9
Firewall 63

9.1 Overview 63
9.1.1 What You Can Do 63
9.1.2 What You Need To Know 63
9.2 General Screen 65
9.3 Service Blocking Screen 65

Chapter 10
Maintenance 69

10.1 Overview 69
10.2 What You Can Do 69
10.3 General Screen 69
10.4 Password Screen 70
10.5 Time Setting Screen 71
10.6 Firmware Upgrade Screen 72
10.7 Configuration Backup/Restore Screen 74
10.8 Restart Screen 75
10.9 Language Screen 75

Chapter 11
Troubleshooting 77

11.1 Overview 77
11.2 Power, Hardware Connections, and LEDs 77
11.3 WAH7130 Access and Login 78
11.4 Internet Access 79
11.5 Wireless LAN Connections 80

Appendix A Common Services 83

Appendix B Pop-up Windows, JavaScript and Java Permissions 87

Appendix C Legal Information 97

Index 103

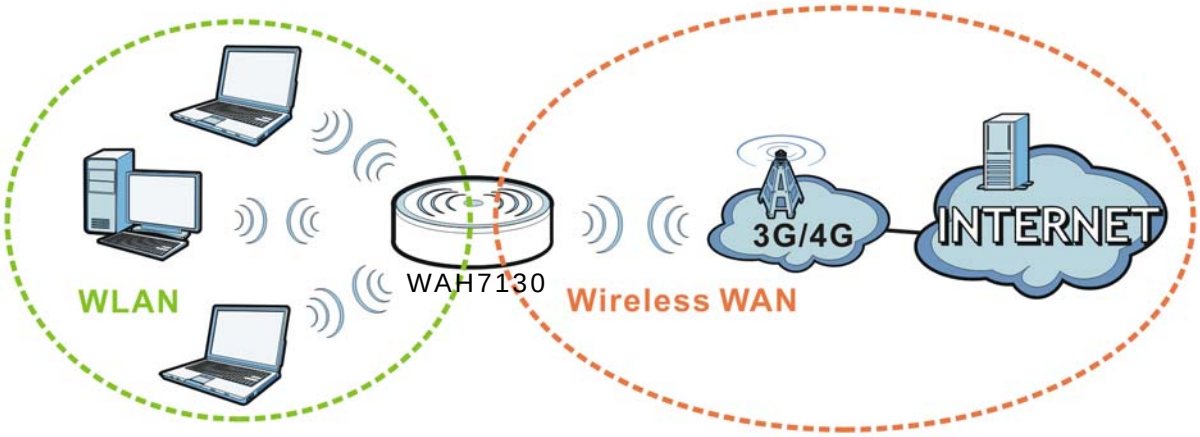
PART I
User's Guide

1 Introduction

1.1 Overview

This chapter introduces the main features and applications of the WAH7130.

The WAH7130 is a wireless router, which can connect to a mobile network and the Internet through a wireless WAN connection and provide easy network access to mobile users without additional wiring. You can set up a wireless network with other IEEE 802.11b/g/n compatible devices.



A range of services such as a firewall are also available for secure Internet computing.

1.2 Ways to Manage the WAH7130

Use any of the following methods to manage the WAH7130.

- WPS (Wi-Fi Protected Setup). You can use the WPS button or the WPS section of the Web Configurator to set up a wireless network with your WAH7130.
- Web Configurator. This is recommended for everyday management of the WAH7130 using a (supported) web browser.

1.3 Good Habits for Managing the WAH7130

Do the following things regularly to make the WAH7130 more secure and to manage the WAH7130 more effectively.

- Change the system login password and wireless security key. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the WAH7130 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the WAH7130. You could simply restore your last configuration.

1.4 Hardware Installation

See your Quick Start Guide for information on making hardware installation. You need to insert a SIM card, install the battery and charge the battery before you can use the WAH7130.

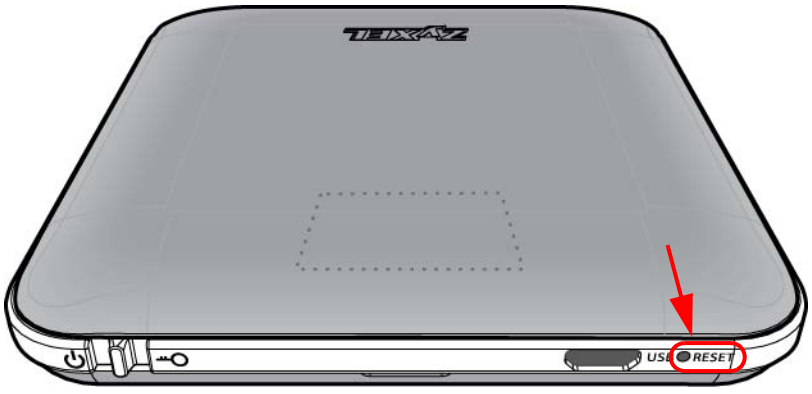
1.5 Resetting the WAH7130

If you forget your password or IP address, or you cannot access the Web Configurator, you will need to use the **RESET** button at the side of the WAH7130 to reload the factory-default configuration file. This means that you will lose all configurations that you had previously saved, the password will be reset to "1234" and the IP address will be reset to "192.168.1.1".

1.5.1 How to Use the RESET Button

1 Make sure the LED is on (not blinking).

2 Press the **RESET** button for five to eight seconds to set the WAH7130 back to its factory-default configurations.



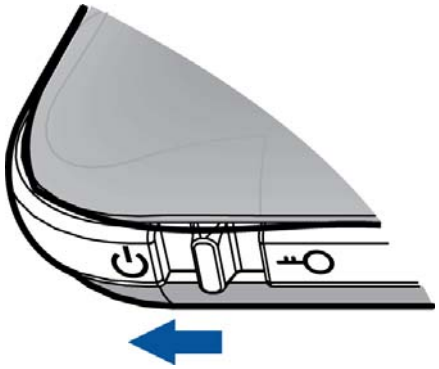
1.6 The Power/WPS Switch

You can use the power/WPS switch of the WAH7130 to turn on or turn off the device, set the WAH7130 to enter sleep mode, wake up the device, or turn on the OLED display. You can also use the switch to activate WPS to set up a wireless network with other WPS-enabled devices.

1.6.1 Turn on/off the WAH7130

To turn on the device, slide the power switch to the power icon and hold until the ZyXEL logo displays in the OLED screen.

To turn off the device, slide the power key to the power icon and hold until the power off icon displays in the OLED screen.



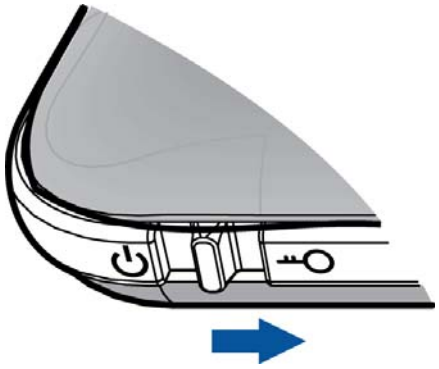
1.6.2 Enter Sleep/Normal Mode

You can set the WAH7130 to be in sleep mode or normal mode using the power switch.

When the WAH7130 is in sleep mode, Wi-Fi will be disabled and the mobile data connection will be disconnected. To have the WAH7130 enter sleep mode, make sure the OLED display is on, slide the power switch to the WPS icon and release.

Note: When the WAH7130 is in sleep mode, wireless clients will not be able to detect and connect to the WAH7130.

To get the WAH7130 back to normal mode, turn on the OLED display, slide the power switch to the WPS icon and release.



1.6.3 Enable the OLED Display

The WAH7130 (in normal mode) automatically disables the OLED display to save battery power when the USB port is not connected and there is no wireless clients associating with the WAH7130. To turn on the OLED display, slide the power switch to the power icon and release.

1.6.4 Enable WPS

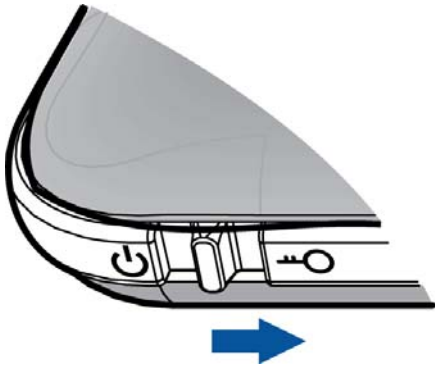
Your WAH7130 supports WiFi Protected Setup (WPS), which is an easy way to set up a secure wireless network. WPS is an industry standard specification, defined by the WiFi Alliance.

WPS allows you to quickly set up a wireless network with strong security, without having to configure security settings manually. Each WPS connection works between two devices. Both devices must support WPS (check each device's documentation to make sure).

Depending on the devices you have, you can either press a button (on the device itself, or in its configuration utility) or enter a PIN (a unique Personal Identification Number that allows one device to authenticate the other) in each of the two devices. When WPS is activated on a device, it has two minutes to find another device that also has WPS activated. Then, the two devices connect and set up a secure network by themselves.

You can use the power/WPS switch to activate WPS in order to quickly set up a wireless network with strong security.

1. Make sure the LED is on (not blinking).
2. Slide the power/WPS switch to the WPS icon and hold for two or three seconds and release it. Press the WPS button on another WPS-enabled device within range of the WAH7130.

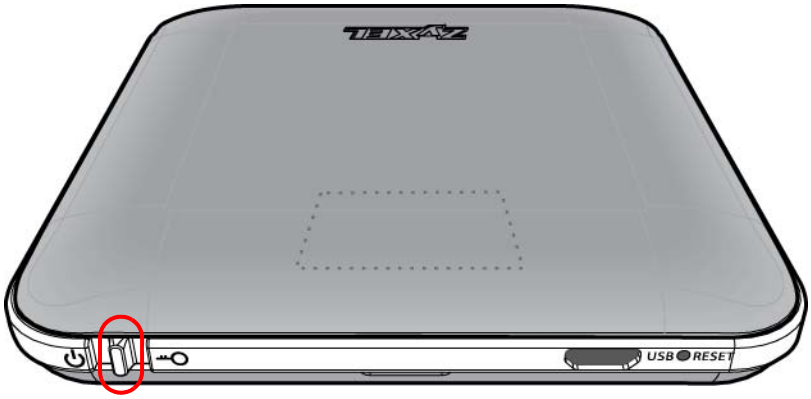


2 ~ 3 seconds

Note: You must activate WPS in the WAH7130 and in another wireless device within two minutes of each other.

1.7 LED

Figure 1 WAH7130 LED



The following table describes the LED.

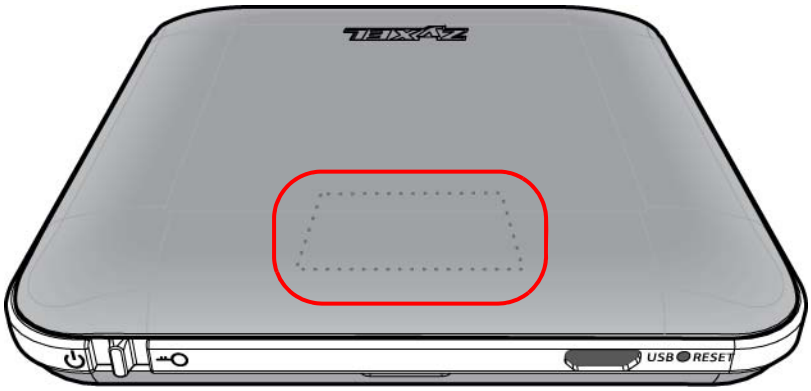
Table 1 WAH7130 LED

COLOR	STATUS	DESCRIPTION
Green	On	The WAH7130 is on and functioning properly.
	Slow Blinking	The WAH7130's battery is being charged.
	Fast Blinking	The WAH7130 is sending/receiving data through the mobile data connection.
Red	On	The WAH7130 has no data connection.
	Blinking	The WAH7130's battery is running low and not being charged.
Orange	On	The WAH7130 is in the process of starting up or turning off.
	Blinking	Firmware upgrade is in progress.
Off		The WAH7130 is turned off.

1.8 OLED Icons

When the OLED display is turned on, you can check the icons display in the OLED screen to see the connection status, battery life and signal strength.

Figure 2 WAH7130 OLED Display



The following table describes the OLED icons.

Table 2 WAH7130 OLED Icons

ICONS	DESCRIPTION
	There is no SIM card inserted.
	The SIM card is inserted improperly or the PIN code is incorrect.
	The the mobile data connection is disconnected because no SIM card is inserted or the PIN code is incorrect.
	The WAH7130 fails to establish a data connection. The APN, user name and/or password may be wrong.
	The the mobile data connection is up.
	The WAH7130 is trying to bring the mobile data connection up
	The type of the mobile network to which the WAH7130 is connecting.
	The SIM card is blocked by your ISP. Get a PUK code from the ISP to enable the SIM card.
	The more bars that display, the stronger the signal strength.
	The signal strength when the WAH7130 is roaming.
	The battery is getting low.
	The battery is being charged.
	The battery is fully charged.
	The battery cannot be charged. If the battery temperature gets too high, remove the battery for a few moments and then reinsert it.
	New firmware is available.
	Firmware upload is in progress.
	Firmware upload failed.
	There are new SMS text messages.
	The SMS box on the WAH7130 is full.
	The number of wireless clients which are currently connecting to the WAH7130.
	The WAH7130 is in the process of turning off.

2

Introducing the Web Configurator

2.1 Overview

This chapter describes how to access the WAH7130 Web Configurator and provides an overview of its screens.

The Web Configurator is an HTML-based management interface that allows easy setup and management of the WAH7130 via Internet browser. Use Internet Explorer 6.0 and later versions, Mozilla Firefox 3 and later versions, or Safari 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the Web Configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Refer to the Troubleshooting chapter (Chapter 11 on page 77) to see how to make sure these functions are allowed in Internet Explorer.

2.2 Accessing the Web Configurator

1. Wirelessly connect your computer to the WAH7130 (refer to the Quick Start Guide).
2. Launch your web browser.
3. Type "http://192.168.1.1" as the website address.

   Your computer must be in the same subnet in order to access this website address.

2.2.1 Login Screen

The Web Configurator initially displays the following login screen.

Figure 3 Login screen

The following table describes the labels in this screen.

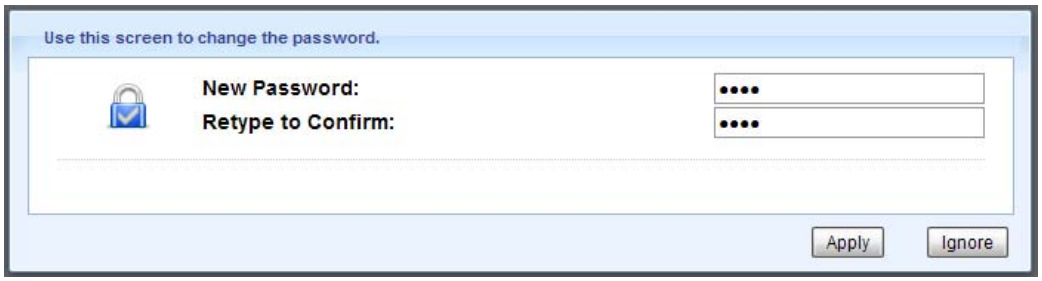
Table 3 Login screen

LABEL	DESCRIPTION
Language	Select the language you want to use to configure the Web Configurator.
Password	Type "1234" (default) as the password. Click **Login**.
	This shows the current signal strength. displays when there is no SIM card inserted. displays when the SIM card is inserted improperly or the PIN code is incorrect. displays when the WAH7130 has been registered and successfully connected to a currently available mobile network. displays when the WAH7130 is registered and successfully connected to another service provider's mobile network using roaming.
	This shows the mobile data connection status. displays when the WAH7130 is trying to bring the mobile data connection up. displays when the mobile data connection is up. displays when there is no SIM card inserted or the PIN code is incorrect. displays when the WAH7130 fails to have a data connection.
	This shows the current battery level or whether the battery is being charged.

2.2.2 Password Screen

You should see a screen asking you to change your password (highly recommended) as shown next.

Figure 4 Change Password Screen



The following table describes the labels in this screen.

Table 4 Change Password Screen

LABEL	DESCRIPTION
New Password	Type a new password.
Retype to Confirm	Retype the password for confirmation.
Apply	Click **Apply** to save your changes back to the WAH7130.
Ignore	Click **Ignore** if you do not want to change the password this time.

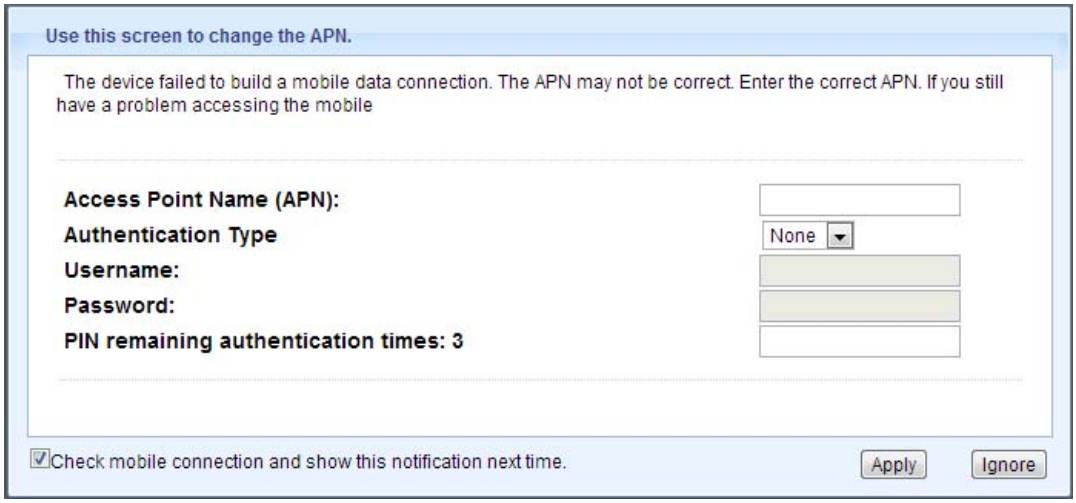
Note: The management session automatically times out when the time period set in the **Administrator Inactivity Timer** field expires (default five minutes; go to Chapter 10 on page 69 to change this). Simply log back into the WAH7130 if this happens.

2.2.3 APN Screen

If the WAH7130 has a SIM card inserted but fails to connect to a mobile network, you should see a screen asking you to change your APN, user name and/or password after logging into the Web Configurator.

Note: This screen will not display when there is no SIM card installed in the WAH7130 or the mobile data connection is up.

Figure 5 Change APN Screen


Use this screen to change the APN.
The device failed to build a mobile data connection. The APN may not be correct. Enter the correct APN. If you still have a problem accessing the mobile
Access Point Name (APN):
Authentication Type
None
Username:
Password:
PIN remaining authentication times: 3
Check mobile connection and show this notification next time.
Apply
Ignore

The following table describes the labels in this screen.

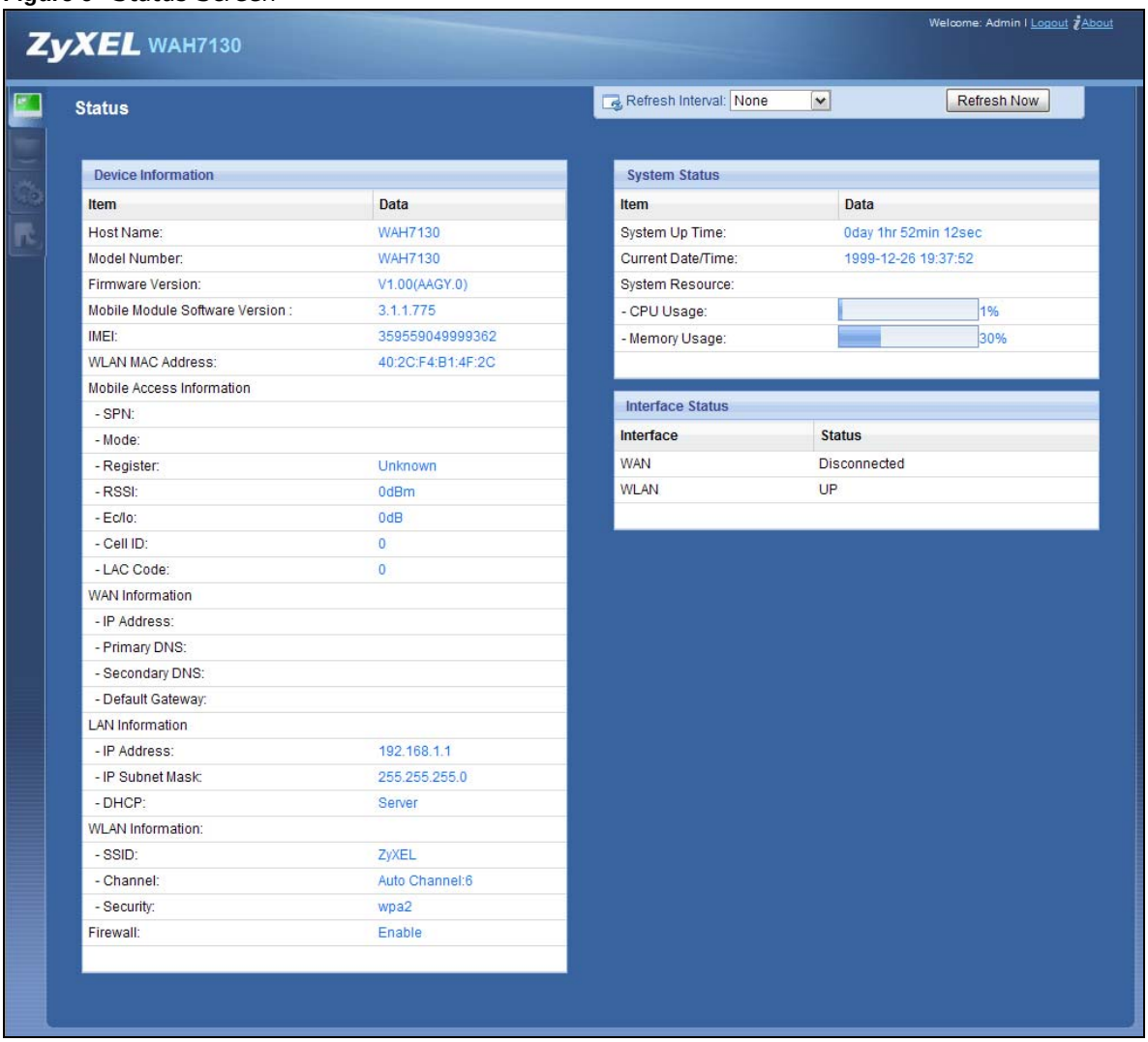
Table 5 Change APN Screen

LABEL	DESCRIPTION
Access Point Name (APN)	Enter the Access Point Name (APN) ("Internet" for example) provided by your service provider.
Authentication Type	Select an authentication protocol (**CHAP** or **PAP**) or **NONE**. Contact your service provider for the correct authentication type. CHAP is more secure than PAP; however, PAP is readily available on more platforms.
Username	Type the user name (of up to 31 printable ASCII characters) given to you by your service provider.
Password	Type the password (of up to 31 printable ASCII characters) associated with the user name above.
PIN remaining authentication times: 3	This field displays when PIN code authentication is enabled. A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card. Enter the 4-digit PIN code (0000 for example) provided by your ISP. Note: If you enter the PIN code incorrectly three times, the SIM card will be blocked by your ISP and you cannot use the account to access the Internet.
Apply	Click **Apply** to save your changes back to the WAH7130.
Ignore	Click **Ignore** if you do not want to change the password this time.

2.3 Status Screen

Click to open the status screen.

Figure 6 Status Screen



The following table describes the icons shown in the **Status** screen.

Table 6 Status Screen Icon Key

ICON	DESCRIPTION
Logout	Click this at any time to exit the Web Configurator.
About	Click this icon to view copyright and a link for related product information.
Refresh Interval: None	Select a number of seconds or **None** from the drop-down list box to refresh all screen statistics automatically at the end of every time interval or to not refresh the screen statistics.
Refresh Now	Click this button to refresh the status screen statistics.
	Click this icon to see the **Status** page. The information in this screen depends on the device mode you select.
	Click this icon to see the **Monitor** navigation menu.
	Click this icon to see the **Configuration** navigation menu.
	Click this icon to see the **Maintenance** navigation menu.

The following table describes the labels shown in the **Status** screen.

Table 7 Status Screen

LABEL	DESCRIPTION
Device Information	
Host Name	This is the **System Name** you enter in the **Maintenance** > **General** screen. It is for identification purposes.
Model Number	This is the model name of your device.
Firmware Version	This is the version of the firmware currently installed in the WAH7130.
Mobile Module Software Version	This displays the version of the firmware currently used in the mobile module.
IMEI	This displays the International Mobile Equipment Number (IMEI) which is the serial number of a mobile device (the WAH7130). IMEI is a unique 15-digit number used to identify a mobile device.
WLAN MAC Address	This shows the wireless LAN MAC Address of your device.
Mobile Access Information	
SPN	This displays the Service Provider Name (SPN).
Mode	This shows the type of the mobile network (such as LTE, UMTS, GSM, HSPA+, etc.) to which the WAH7130 is connecting.
Register	This shows the WAH7130's registration status. • **Registered(Home network)** when the WAH7130 has been registered and successfully connected to your service provider's network. • **Not registered/Actively searching** when the WAH7130 has not registered yet and is looking for an available network. • **Not registered/Not searching** when the WAH7130 is not registered yet and has stopped searching for an available network. • **Registration denied** when the WAH7130 has failed to register with a mobile network. It shows **Unknown** when the WAH7130 has no SIM card installed or **Roaming** when the WAH7130 is using roaming.
RSSI	This shows the received signal strength indicator (RSSI), that is, the received signal strength in dBm.
Ec/Io	This shows the ratio (in dB) of the received energy per chip and the interference level.
Cell ID	This shows the unique number which is used to identify a cell within the mobile network.
LAC Code	This shows the Location Area Code (LAC), a unique number assigned to a set of base stations. The location area code is broadcast by each base station.
WAN Information	
IP Address	This shows the WAH7130's WAN IP address.
Primary DNS	This shows the first DNS server address assigned by the ISP.
Secondary DNS	This shows the second DNS server address assigned by the ISP.
Default Gateway	This shows the gateway IP address assigned by the ISP.
LAN Information	
IP Address	This shows the WAH7130's LAN IP address.
IP Subnet Mask	This shows the WAH7130's subnet mask in the LAN.
DHCP	This field displays what DHCP services the WAH7130 is providing to the LAN. Choices are: **Server** - The WAH7130 acts as a DHCP server and assigns IP addresses to other computers in the LAN. **None** - The WAH7130 is not providing any DHCP services to the LAN.
WLAN Information	

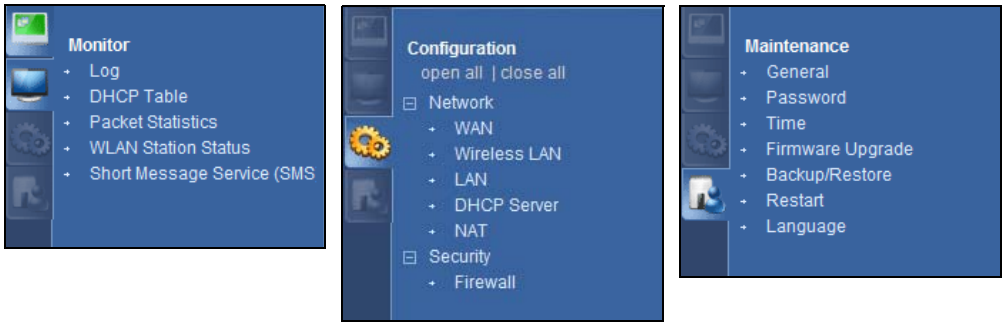
Table 7 Status Screen (continued)

LABEL	DESCRIPTION
SSID	This shows a descriptive name used to identify the WAH7130 in the wireless LAN.
Channel	This shows the channel number which you select manually.
Security	This shows the level of wireless security the WAH7130 is using.
Firewall	This shows whether the firewall is enabled or not.
System Status	
Item	This column shows the type of data the WAH7130 is recording.
Data	This column shows the actual data recorded by the WAH7130.
System Up Time	This is the total time the WAH7130 has been on.
Current Date/Time	This field displays your WAH7130's present date and time.
System Resource	
- CPU Usage	This displays what percentage of the WAH7130's processing ability is currently used. When this percentage is close to 100%, the WAH7130 is running at full load, and the throughput is not going to improve anymore. If you want some applications to have more throughput, you should turn off other applications (for example, using bandwidth management.)
- Memory Usage	This shows what percentage of the heap memory the WAH7130 is using.
Cellular Data Usage	This field displays what percentage of the monthly quota has bee used and the date on which the statistics were last reset. This field is available only when you enable mobile data usage control.
Interface Status	
Interface	This displays the WAH7130's interface type.
Status	For the WAN, this field displays: • **Connecting** when the WAH7130 is trying to bring the mobile data connection up. • **Connected** when the mobile data connection is up. • **Disconnected** when there is no SIM card inserted or the PIN code is incorrect. • **Connection Error** when the WAH7130 fails to have a data connection. For the WLAN, it displays **Up** when the WLAN is enabled or **Down** when the WLAN is disabled.

2.3.1 Navigation Panel

Use the sub-menus on the navigation panel to configure WAH7130 features.

Figure 7 Navigation Panel: Router Mode



The following table describes the sub-menus.

Table 8 Navigation Panel: Router Mode

LINK	TAB	FUNCTION
Status		This screen shows the WAH7130's general device, system and interface status information.
MONITOR		
Log		Use this screen to view the list of activities recorded by your WAH7130.
DHCP Table		Use this screen to view current DHCP client information.
Packet Statistics		Use this screen to view port status and packet specific statistics.
WLAN Station Status		Use this screen to view the wireless stations that are currently associated to the WAH7130.
Short Message Service (SMS)		Use this screen to view the SMS text messages the WAH7130 received from a mobile device.
CONFIGURATION		
Network		
WAN	Broadband	This screen allows you to configure ISP parameters.
	Data Plan	Use this screen to enable data usage control and set a monthly data limit.
	PIN Setting	Use this screen to configure PIN settings.
	Change PIN	Use this screen to change the SIM card's default PIN code.
Wireless LAN	General	Use this screen to enable the wireless LAN and configure wireless LAN and wireless security settings.
	Guest Wi-Fi	Use this screen to configure multiple BSSs on the WAH7130.
	MAC Filter	Use the MAC filter screen to configure the WAH7130 to block access to devices or block the devices from accessing the WAH7130.
LAN	IP	Use this screen to configure LAN IP address and subnet mask.
DHCP Server	General	Use this screen to enable the WAH7130's DHCP server.
	Client List	Use this screen to view information related to your DHCP status.
NAT	General	Use this screen to enable NAT.
	Port Forwarding	Use this screen to configure servers behind the WAH7130 and forward incoming service requests to the server(s) on your local network.
Security		
Firewall	General	Use this screen to activate/deactivate the firewall.
	Service Blocking	This screen shows a summary of the firewall rules, and allows you to edit/ add a firewall rule.
MAINTENANCE		
General	General	Use this screen to view and change administrative settings such as system and domain names.
Password	Password Setup	Use this screen to change the password of your WAH7130.
Time	Time Setting	Use this screen to change your WAH7130's time and date.
Firmware Upgrade	Firmware Upgrade	Use this screen to upload firmware to your WAH7130.
Backup/ Restore	Backup/ Restore	Use this screen to backup and restore the configuration or reset the factory defaults to your WAH7130.
Restart	System Restart	This screen allows you to reboot the WAH7130 without turning the power off.
Language	Language	This screen allows you to select the language you prefer.

PART II
Technical Reference

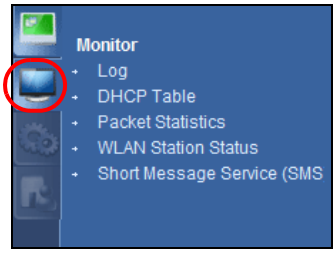
3

Monitor

3.1 Overview

This chapter discusses read-only information related to the device state of the WAH7130.

To access the **Monitor** screens, click .



3.2 What You Can Do

- Use the **Log** screen to see the logs for the activity on the WAH7130 (Section 3.3 on page 27).
- Use the **DHCP Table** screen to view information related to your DHCP status (Section 3.4 on page 28).
- use the **Packet Statistics** screen to view port status, packet specific statistics, the "system up time" and so on (Section 3.5 on page 29).
- Use the **WLAN Station Status** screen to view the wireless stations that are currently associated to the WAH7130 (Section 3.6 on page 30).
- Use the **Short Message Service (SMS)** screen to view and manage the text messages the WAH7130 received from mobile devices or the service provider (Section 3.7 on page 31).

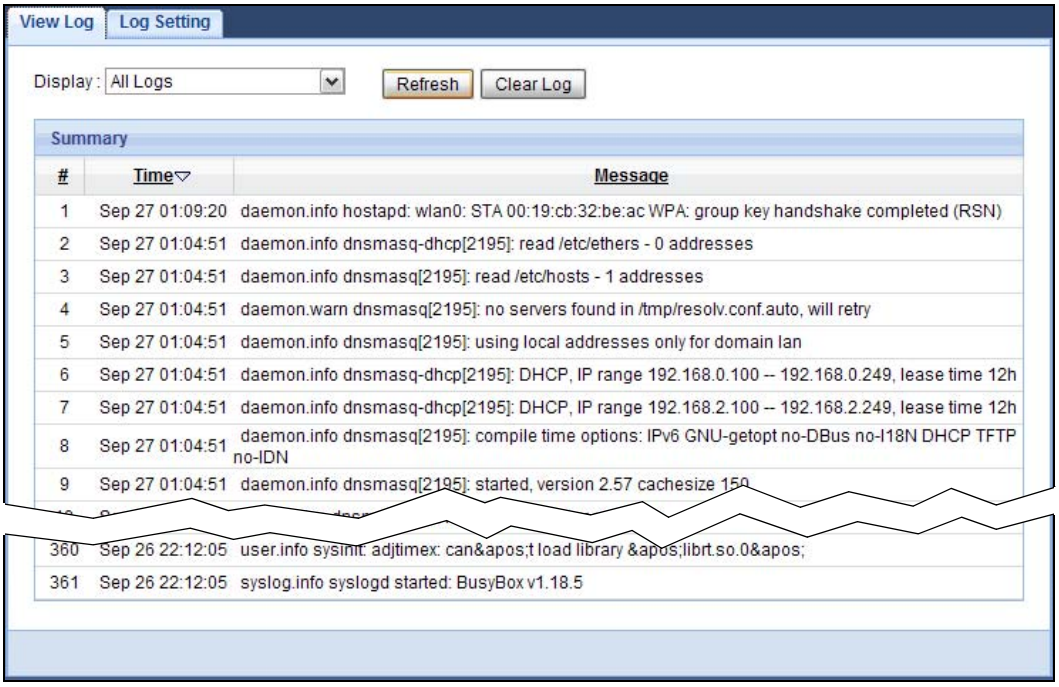
3.3 The Log Screen

The Web Configurator allows you to look at all of the WAH7130's logs in one location.

3.3.1 View Log

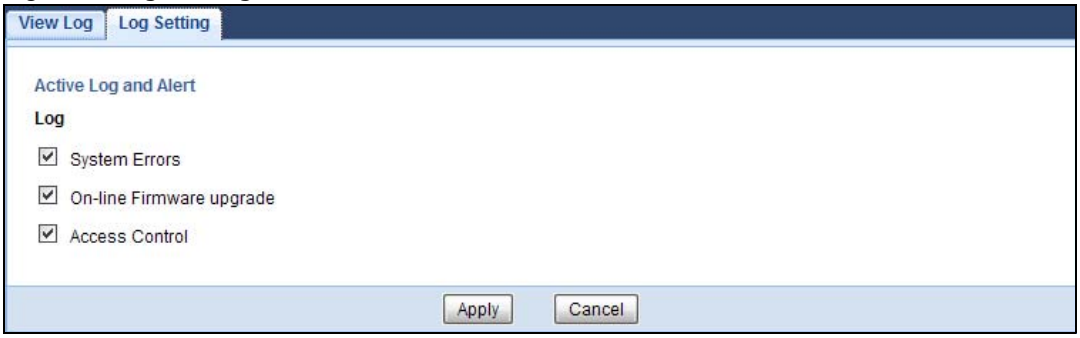
Use the **View Log** screen to see the logged messages for the WAH7130. The log wraps around and deletes the old entries after it fills. Select what logs you want to see from the **Display** drop list. The log choices depend on your settings in the **Log Setting** screen. Click **Refresh** to renew the log screen. Click **Clear Log** to delete all the logs.

Figure 8 View Log


View Log
Log Setting
Display : All Logs
Refresh
Clear Log
Summary
Time Message
1 Sep 27 01:09:20 daemon.info hostapd: wlan0: STA 00:19:cb:32:be:ac WPA: group key handshake completed (RSN)
2 Sep 27 01:04:51 daemon.info dnsmasq-dhcp[2195]: read /etc/ethers - 0 addresses
3 Sep 27 01:04:51 daemon.info dnsmasq[2195]: read /etc/hosts - 1 addresses
4 Sep 27 01:04:51 daemon.warn dnsmasq[2195]: no servers found in /tmp/resolv.conf.auto, will retry
5 Sep 27 01:04:51 daemon.info dnsmasq[2195]: using local addresses only for domain lan
6 Sep 27 01:04:51 daemon.info dnsmasq-dhcp[2195]: DHCP, IP range 192.168.0.100 -- 192.168.0.249, lease time 12h
7 Sep 27 01:04:51 daemon.info dnsmasq-dhcp[2195]: DHCP, IP range 192.168.2.100 -- 192.168.2.249, lease time 12h
8 Sep 27 01:04:51 daemon.info dnsmasq[2195]: compile time options: IPv6 GNU-getopt no-DBus no-I18N DHCP TFTP no-IDN
9 Sep 27 01:04:51 daemon.info dnsmasq[2195]: started, version 2.57 cachesize 150
360 Sep 26 22:12:05 user.info sysinit: adjtimex: can't load library 'librt.so.0'
361 Sep 26 22:12:05 syslog.info syslogd started: BusyBox v1.18.5

You can configure which logs to display in the **View Log** screen. Go to the **Log Setting** screen and select the logs you wish to display. Click **Apply** to save your settings. Click **Cancel** to start the screen afresh.

Figure 9 Log Settings

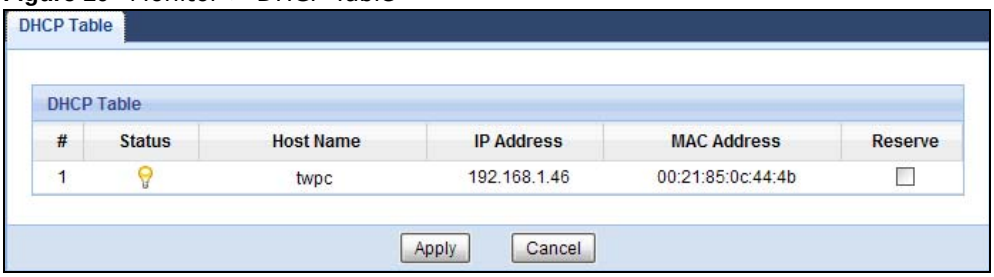


3.4 DHCP Table

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the WAH7130's LAN as a DHCP server or disable it. When configured as a server, the WAH7130 provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on that network, or else the computer must be manually configured.

Click **Monitor > DHCP Table** or **Configuration > Network > DHCP Server > Client List**. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP client information (including **MAC Address**, and **IP Address**) of all network clients using the WAH7130's DHCP server.

Figure 10 Monitor > DHCP Table



The following table describes the labels in this screen.

Table 9 Summary: DHCP Table

LABEL	DESCRIPTION
#	This is the index number of the host computer.
Status	This field displays whether the connection to the host computer is up (a yellow bulb) or down (a gray bulb).
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Reserve	Select this if you want to reserve the IP address for this specific MAC address.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

3.5 Packet Statistics

Click **Monitor > Packet Statistics**. Read-only information here includes port status, packet specific statistics and the "system up time". The **Poll Interval(s)** field is configurable and is used for refreshing the screen.

Figure 11 Packet Statistics

Packet Statistics
Packet Statistics
Port Status TxPkts RxPkts Collisions Tx Mbyte Rx Mbyte
WAN UP 44 39 0 1 1
WLAN UP 3103 2945 0 2 1
System Up Time : 00: 06: 04
Poll Interval(s) : None
Set Interval
Stop

The following table describes the labels in this screen.

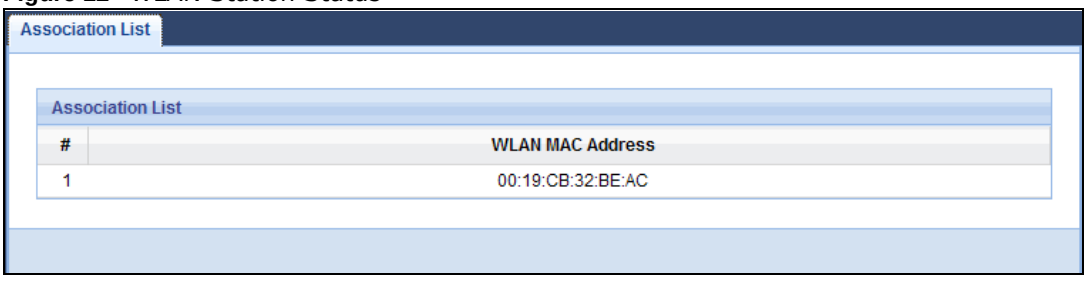
Table 10 Packet Statistics

LABEL	DESCRIPTION
Port	This is the WAH7130's interface type.
Status	For the WAN, it displays **Up** when the mobile data connection is up, **Connecting** when the WAH7130 is trying to bring the mobile data connection up, and displays **Down** when the 3G/4G connection is down or not activated. For the WLAN, it displays **Up** when the WLAN is enabled and **Down** when the WLAN is disabled.
TxPkts	This is the number of transmitted packets on this interface.
RxPkts	This is the number of received packets on this interface.
Collisions	This is the number of collisions on this interface.
Tx Mbyte	This displays the total amount of data in Megabytes that has been transmitted on this interface since the WAH7130 last restarted.
Rx Mbyte	This displays the total amount of data in Megabytes that has been received on this interface since the WAH7130 last restarted.
System Up Time	This is the total time the WAH7130 has been on.
Poll Interval(s)	Enter the time interval in seconds for refreshing statistics in this field.
Set Interval	Click this button to apply the new poll interval you entered in the **Poll Interval(s)** field.
Stop	Click **Stop** to stop refreshing statistics.

3.6 WLAN Station Status

Click **Monitor > WLAN Station Status**. View the wireless stations that are currently associated to the WAH7130 in the **Association List**. Association means that a wireless client (for example, your network or computer with a wireless network card) has connected successfully to the AP (or wireless router) using the same SSID, channel and security settings.

Figure 12 WLAN Station Status



The following table describes the labels in this screen.

Table 11 WLAN Station Status

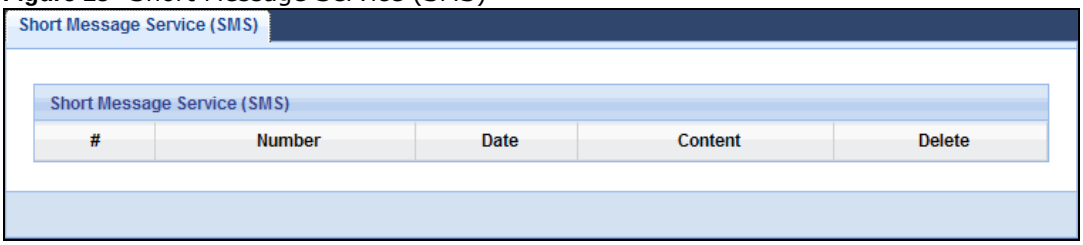
LABEL	DESCRIPTION
#	This is the index number of an associated wireless station, such as your notebook or smartphone.
WLAN MAC Address	This field displays the MAC address of an associated wireless station.

3.7 Short Message Service (SMS)

Click **Monitor > Short Message Service (SMS)**. View the text messages that the WAH7130 received from mobile devices or the service provider.

When the SMS box is full the WAH7130 will begin to delete older entries as it adds new ones.

Figure 13 Short Message Service (SMS)



The following table describes the labels in this screen.

Table 12 Short Message Service (SMS)

LABEL	DESCRIPTION
#	This is the index number of each message.
Number	This is the mobile phone number from which the message is sent.
Date	This is the date and time the message was received.
Content	This is the content of the message.
Delete	Click this to remove the message from the WAH7130 SMS box.

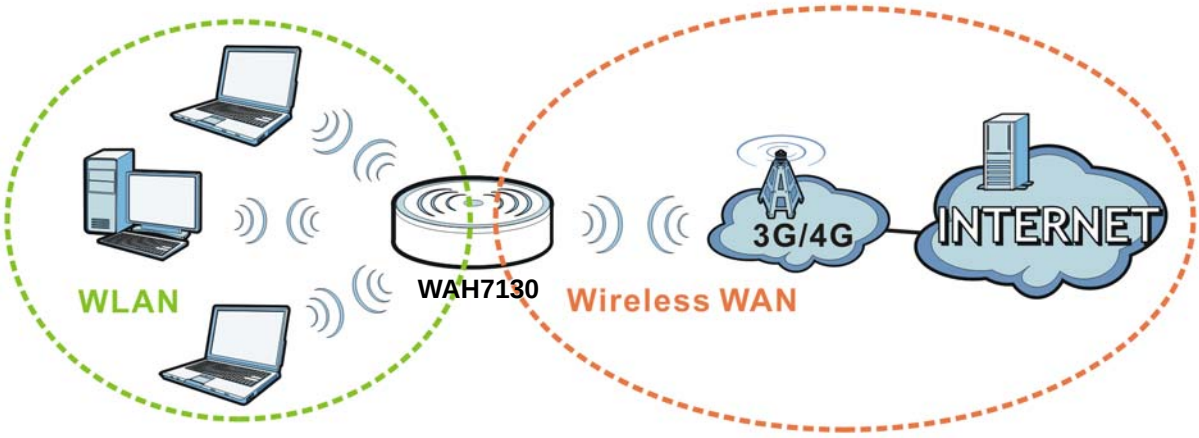
4 WAN

4.1 Overview

This chapter discusses the WAH7130's **WAN** screens. Use these screens to configure your WAH7130 for Internet access.

A wireless WAN (WWAN) and a wireless LAN (WLAN) are both wireless networks. A WLAN uses Wi-Fi to transfer data in a private network, while a WWAN can use mobile telecommunication technologies to provide access to a service provider's mobile network and the Internet. The WAH7130 supports both WLAN and WWAN to allow Wi-Fi devices in the WLAN to surf the Internet, check e-mail and communicate with other networking devices outside the coverage of the WLAN.

Figure 14 Wireless LAN and Wireless WAN



4.2 What You Can Do

- Use the **Broadband** screen to enter your ISP information (Section 4.4 on page 35).
- Use the **Data Plan** screen to set a monthly limit on the total traffic (Section 4.5 on page 36).
- Use the **PIN Setting** screen to enable PIN authentication and configure the PIN code, or enter the PUK code when the SIM card is blocked (Section 4.6 on page 37).
- Use the **Change PIN** screen to change the default PIN code (Section 4.4 on page 35).

4.3 What You Need To Know

The information in this section can help you configure the screens for your 3G/4G LTE connection.

3G

3G (Third Generation) is a digital, packet-switched wireless technology. Bandwidth usage is optimized as multiple users share the same channel and bandwidth is only allocated to users when they send data. It allows fast transfer of voice and non-voice data and provides broadband Internet access to mobile devices.

4G

4G is the fourth generation of the mobile telecommunications technology and a successor of 3G. Both the WiMAX and Long Term Evolution (LTE) standards are the 4G candidate systems. 4G only supports all-IP-based packet-switched telephony services and is required to offer gigabit speed access.

Note: The actual data rate you obtain varies depending on your mobile environment. The environmental factors may include the number of mobile devices which are currently connected to the mobile network, the signal strength to the mobile network, and so on.

See the following table for a comparison between mobile telecommunications technologies.

Table 13 Mobile Telecommunications Technologies/Standards

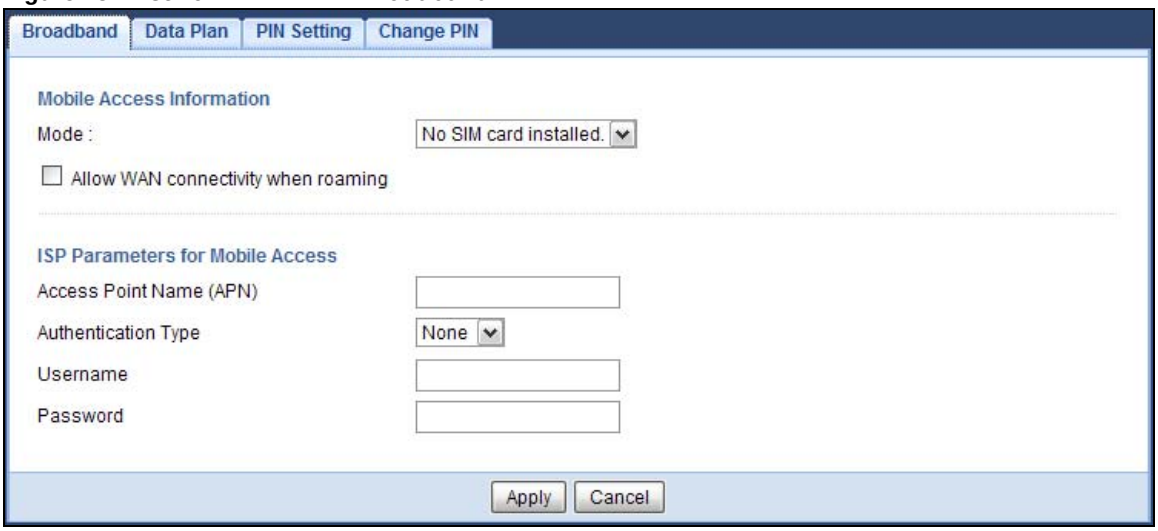
NAME	TYPE	MOBILE PHONE AND DATA STANDARDS		DATA SPEED
		GSM-BASED	CDMA-BASED	
2G	Circuit-switched	GSM (Global System for Mobile Communications), Personal Handy-phone System (PHS), etc.	Interim Standard 95 (IS-95), the first CDMA-based digital cellular standard pioneered by Qualcomm. The brand name for IS-95 is cdmaOne. IS-95 is also known as TIA-EIA-95.	Slow
2.5G	Packet-switched	GPRS (General Packet Radio Services), High-Speed Circuit-Switched Data (HSCSD), etc.	CDMA2000 is a hybrid 2.5G / 3G protocol of mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio.	
2.75G	Packet-switched	Enhanced Data rates for GSM Evolution (EDGE), Enhanced GPRS (EGPRS), etc.	CDMA2000 1xRTT (1 times Radio Transmission Technology) is the core CDMA2000 wireless air interface standard. It is also known as 1x, 1xRTT, or IS-2000 and considered to be a 2.5G or 2.75G technology.	
3G	Packet-switched	UMTS (Universal Mobile Telecommunications System), a third-generation (3G) wireless standard defined in ITU[A] specification, is sometimes marketed as 3GSM. The UMTS uses GSM infrastructures and W-CDMA (Wideband Code Division Multiple Access) as the air interface.	CDMA2000 EV-DO (Evolution-Data Optimized, originally 1x Evolution-Data Only), also referred to as EV-DO, EVDO, or just EV, is an evolution of CDMA2000 1xRTT and enables high-speed wireless connectivity. It is also denoted as IS-856 or High Data Rate (HDR).	
3.5G	Packet-switched	HSDPA (High-Speed Downlink Packet Access) is a mobile telephony protocol, used for UMTS-based 3G networks and allows for higher data transfer speeds.		
4G/LTE	Packet-switched	The LTE (Long Term Evolution) standard is based on the GSM and UMTS network technologies.		Fast

A. The International Telecommunication Union (ITU) is an international organization within which governments and the private sector coordinate global telecom networks and services.

4.4 Broadband Screen

Use this screen to change your WAH7130's settings for mobile access. Click **Network > WAN** from the **Configuration** menu.

Figure 15 Network > WAN > Broadband



The following table describes the labels in this screen.

Table 14 Network > WAN > Broadband

LABEL	DESCRIPTION
Mobile Access Information	
Mode	This field is not configurable and shows **No SIM card installed.** if there is no SIM card inserted in the WAH7130. Select the type of the network (**4G/LTE only**, **3G/UMTS only**, or **2G/EDGE only**) to which you want the WAH7130 to connect when there is a SIM card inserted. Otherwise, select **Automatically** to have the WAH7130 connect to an available network using the default settings on the SIM card. If the currently registered mobile network is not available or the mobile network's signal strength is too low, the WAH7130 switches to another available mobile network.
Allow WAN connectivity when roaming	3G/4G roaming is to use your mobile device in an area which is not covered by your service provider. Select this option to enable roaming to ensure that your WAH7130 is kept connected to the Internet when you are travelling outside the geographical coverage area of the network to which you are registered.
ISP Parameters for Mobile Access	
Access Point Name (APN)	Enter the Access Point Name (APN) provided by your service provider. Connections with different APNs may provide different services (such as Internet access or MMS (Multi-Media Messaging Service)) and charging method. You can enter up to 31 printable ASCII characters. Spaces are allowed.

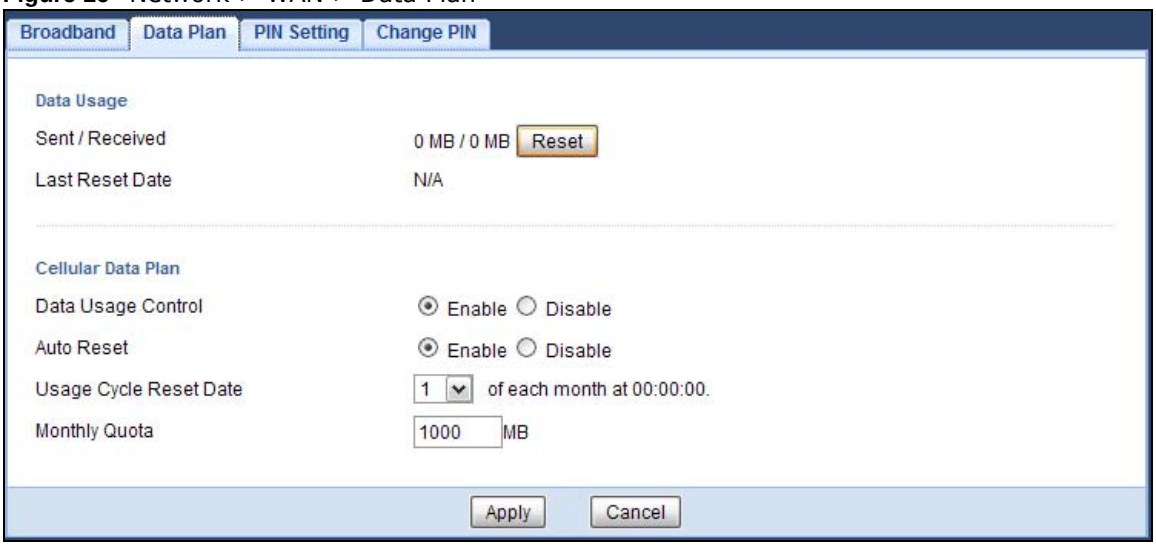
Table 14 Network > WAN > Broadband

LABEL	DESCRIPTION
Authentication	The WAH7130 supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). CHAP is more secure than PAP; however, PAP is readily available on more platforms. Select an authentication protocol (**CHAP** or **PAP**) or **NONE**. Contact your service provider for the correct authentication type.
Username	Type the user name (of up to 31 printable ASCII characters) given to you by your service provider.
Password	Type the password (of up to 31 printable ASCII characters) associated with the user name above.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to begin configuring this screen afresh.

4.5 Data Plan Screen

Use this screen to enable mobile data usage control and set a monthly data limit. Click **Network > WAN > Data Plan** from the **Configuration** menu.

Figure 16 Network > WAN > Data Plan



The following table describes the labels in this screen.

Table 15 Network > WAN > Data Plan

LABEL	DESCRIPTION
Data Usage	
Sent/Received	This shows how much downstream and/or upstream data (in Mega bytes) are transmitted via the mobile data connection.
Reset	Click this to update the data usage statistics.
Last Reset Date	This is the date in which the statistics were last reset.
Cellular Data Plan	

Table 15 Network > WAN > Data Plan (continued)

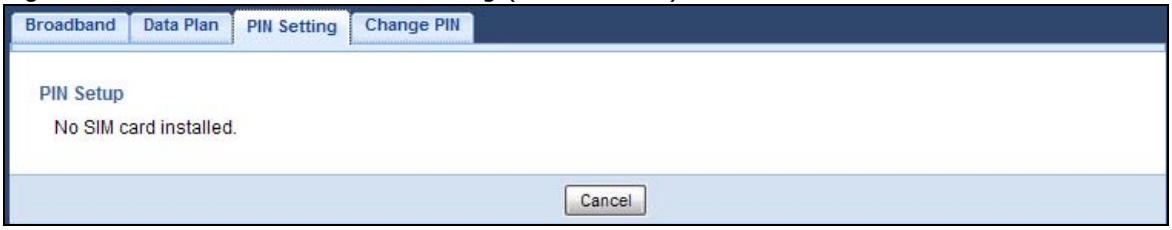
LABEL	DESCRIPTION
Data Usage Control	Select **Enable** to set a monthly limit on the total traffic in both directions for the user account of the installed SIM card. Otherwise, select **Disable** to turn off data usage control.
Auto Reset	Select **Enable** to have the WAH7130 automatically resets the statistics at the specified time. If **Disabled** is selected, you cannot configure the date and the statistics will not be reset.
Usage Cycle Reset Date	Select the date in which the WAH7130 resets the statistics every month. Note: If the date you selected is not available in a month, such as 30th or 31th of February, the WAH7130 resets the statistics on the first day of the next month.
Monthly Quota	Specify how much data (in Mega bytes) can be transmitted via the mobile data connection within one month. Note: If you change the value after you configure and enable data usage control, the WAH7130 resets the statistics.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to begin configuring this screen afresh.

4.6 PIN Setting Screen

To change your WAH7130's PIN settings, click **Network** > **WAN** > **PIN Setting**.

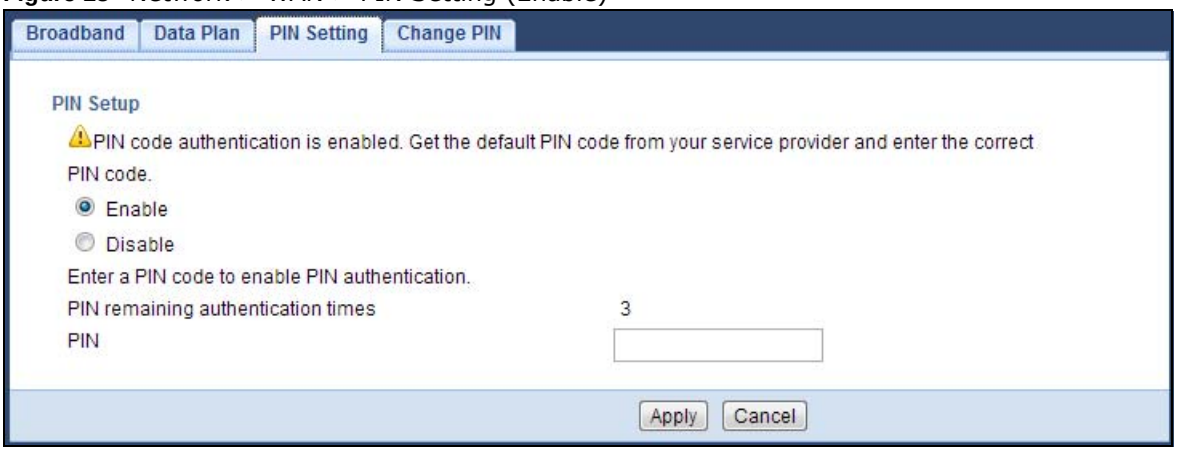
The screen appears as shown if there is no SIM card inserted in the WAH7130.

Figure 17 Network > WAN > PIN Setting (No SIM Card)



The screen appears as shown if PIN code authentication is enabled.

Figure 18 Network > WAN > PIN Setting (Enable)



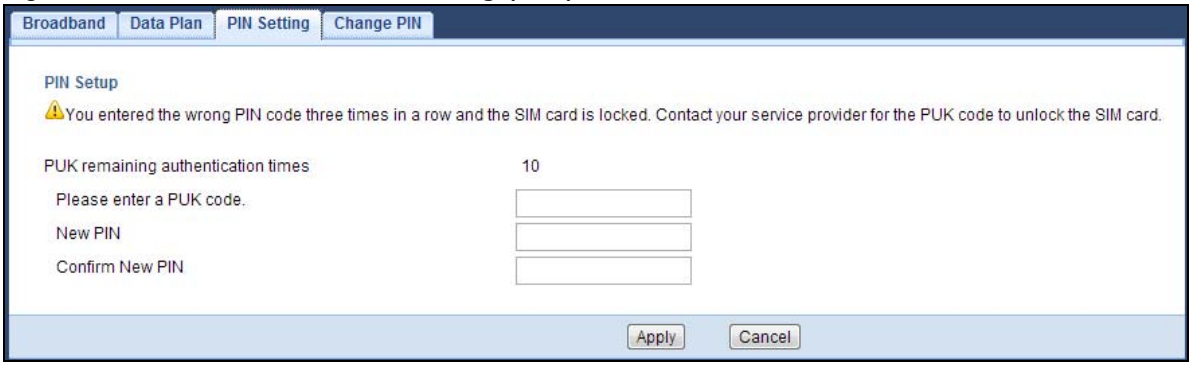
The following table describes the labels in this screen.

Table 16 Network > WAN > PIN Setting

LABEL	DESCRIPTION
PIN Setup	
	Select **Enable** to turn on PIN code authentication. A PIN (Personal Identification Number) code is a key to a SIM card. Without the PIN code, you cannot use the SIM card. Select **Disable** to turn off PIN code authentication.
PIN remaining authentication times	This shows how many times (3 by default) you can enter the PIN code. If you enter the PIN code incorrectly three times, the SIM card will be blocked by your ISP and you cannot use the account to access the Internet. You will need to contact your ISP to get a PUK code.
PIN	If you select **Enable**, enter the 4-digit PIN code (0000 for example) provided by your ISP for the inserted SIM card.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to begin configuring this screen afresh.

The screen appears as shown if the PIN code is entered incorrectly three times.

Figure 19 Network > WAN > PIN Setting (PUK)


Broadband
Data Plan
PIN Setting
Change PIN
PIN Setup
You entered the wrong PIN code three times in a row and the SIM card is locked. Contact your service provider for the PUK code to unlock the SIM card.
PUK remaining authentication times
10
Please enter a PUK code.
New PIN
Confirm New PIN
Apply
Cancel

The following table describes the labels in this screen.

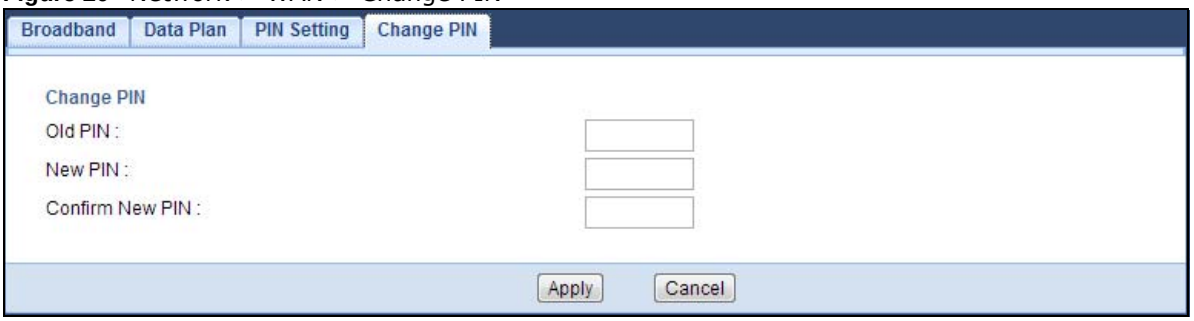
Table 17 Network > WAN > PIN Setting (PUK)

LABEL	DESCRIPTION
PIN Setup	
PUK remaining authentication times	This shows how many times (10 by default) you can enter the PUK code. If an incorrect PUK code is entered 10 times, the SIM card will be disabled permanently. You then need to contact your ISP for a new SIM card.
Please enter a PUK code	If you enter the PIN code incorrectly three times, the SIM card will be blocked by your ISP and you cannot use the account to access the Internet. You should get the PUK (Personal Unblocking Key) code (four to eight digits) from your ISP. Enter the PUK code to enable the SIM card.
New PIN	Configure a PIN code for the SIM card. You can specify any four to eight digits to have a new PIN code or enter the previous PIN code.
Confirm New PIN	Enter the PIN code again for confirmation.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to begin configuring this screen afresh.

4.7 Change PIN Screen

Use this screen to change your SIM card's existing PIN code when there is a SIM card installed in the WAH7130. Click **Network > WAN > Change PIN** from the **Configuration** menu.

Figure 20 Network > WAN > Change PIN



The following table describes the labels in this screen.

Table 18 Network > WAN > Change PIN

LABEL	DESCRIPTION
Change PIN	
Old PIN	Enter the default or existing PIN code for the inserted SIM card.
New PIN	Configure a new PIN code for the SIM card. You can specify any four to eight digits to have a new PIN code.
Confirm New PIN	Enter the new PIN code again for confirmation.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to begin configuring this screen afresh.

5

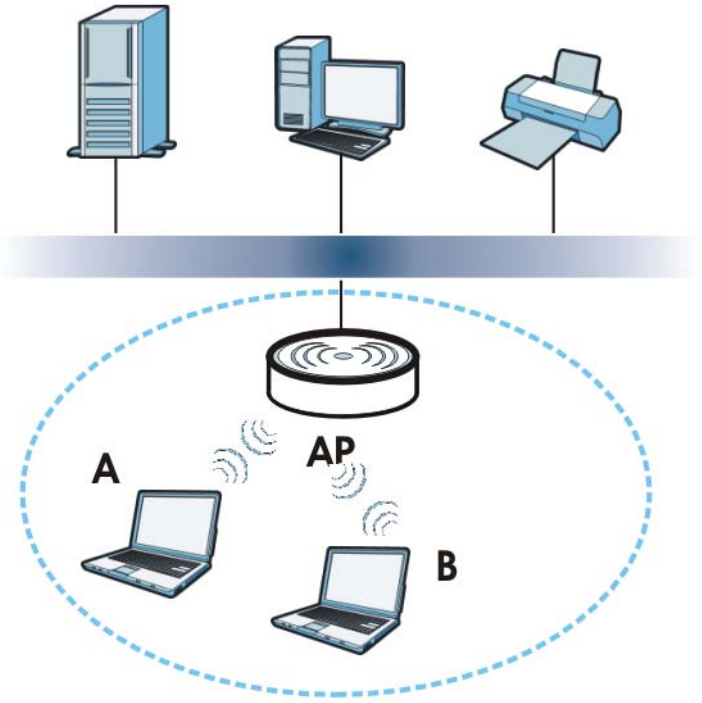
Wireless LAN

5.1 Overview

This chapter discusses how to configure the wireless network settings in your WAH7130. See the appendices for more detailed information about wireless networks.

The following figure provides an example of a wireless network.

Figure 21 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** are called wireless clients. The wireless clients use the access point (AP) to interact with other devices (such as the printer) or with the Internet. Your WAH7130 is the AP.

5.1.1 What You Can Do

- Use the **General** screen to turn the wireless connection on or off, set up wireless security between the WAH7130 and the wireless clients, and make other basic configuration changes (Section 5.2 on page 43).
- Use the **Guest Wi-Fi** screen to set up a second wireless network on your WAH7130 (Section 5.3 on page 45).
- Use the **MAC Filter** screen to allow or deny wireless stations based on their MAC addresses from connecting to the WAH7130 (Section 5.4 on page 46).

5.1.2 What You Should Know

Every wireless network must follow these basic guidelines.

- Every wireless client in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentity.
- If two wireless networks overlap, they should use different channels.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.
- Every wireless client in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

SSID

Normally, the AP acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the AP does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized devices to get the SSID. In addition, unauthorized devices can still see the information that is sent in the wireless network.

MAC Address Filter

Every wireless client has a unique identification number, called a MAC address.[1] A MAC address is usually written using twelve hexadecimal characters[2]; for example, 00A0C5000002 or 00:A0:C5:00:00:02. To get the MAC address for each wireless client, see the appropriate User's Guide or other documentation.

1. Some wireless devices, such as scanners, can detect wireless networks but cannot use wireless networks. These kinds of wireless devices might not have MAC addresses.
2. Hexadecimal characters are 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F.

You can use the MAC address filter to tell the AP which wireless clients are allowed or not allowed to use the wireless network. If a wireless client is allowed to use the wireless network, it still has to have the correct settings (SSID, channel, and security). If a wireless client is not allowed to use the wireless network, it does not matter if it has the correct settings.

This type of security does not protect the information that is sent in the wireless network. Furthermore, there are ways for unauthorized devices to get the MAC address of an authorized wireless client. Then, they can use that MAC address to use the wireless network.

Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

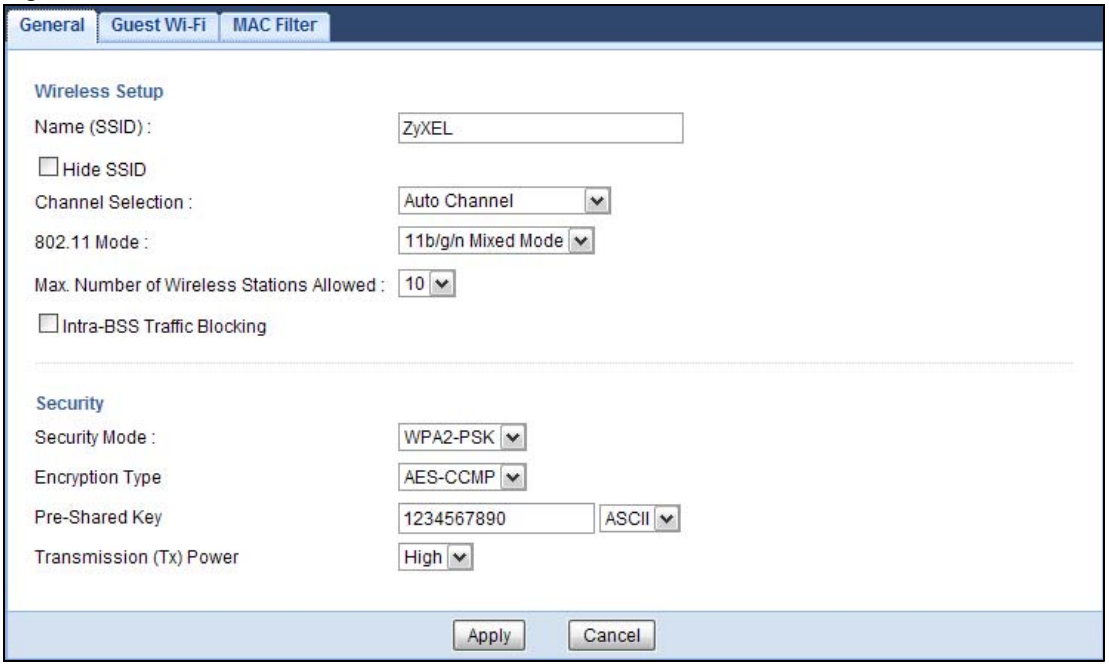
5.2 General Wireless LAN Screen

Use this screen to configure the SSID and wireless security of the wireless LAN.

Note: If you are configuring the WAH7130 from a computer connected to the wireless LAN and you change the WAH7130's SSID, channel or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the WAH7130's new settings.

Click **Network** > **Wireless LAN** to open the **General** screen.

Figure 22 Network > Wireless LAN > General



The following table describes the general wireless LAN labels in this screen.

Table 19 Network > Wireless LAN > General

LABEL	DESCRIPTION
Name (SSID)	The SSID (Service Set IDentity) identifies the Service Set with which a wireless client is associated. Enter a descriptive name (up to 32 printable characters found on a typical English language keyboard) for the wireless LAN.
Hide SSID	Select this check box to hide the SSID in the outgoing beacon frame so a station cannot obtain the SSID through scanning using a site survey tool.
Channel Selection	Set the operating frequency/channel depending on your particular region. Select a channel from the drop-down list box. The options vary depending on the frequency band and the country you are in. Otherwise, select **Auto Channel** to have the WAH7130 automatically choose the channel with the least interference.
802.11 Mode	You can select from the following: • **11b Only**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the WAH7130. In this mode, all wireless devices can only transmit at the data rates supported by IEEE 802.11b. • **11g Only**: allows IEEE 802.11g compliant WLAN devices to associate with the Device. IEEE 802.11b compliant WLAN devices can associate with the WAH7130 only when they use the short preamble type. • **11b/g Mixed Mode**: allows either IEEE 802.11b or IEEE 802.11g compliant WLAN devices to associate with the WAH7130. The WAH7130 adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. • **11 b/g/n Mixed Mode**: allows IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the WAH7130. The transmission rate of your WAH7130 might be reduced.
Max. Number of Wireless Stations Allowed	Select a number (from 1 to 10) to limit the number of wireless clients which can access your wireless network.
Intra-BSS Traffic Blocking	A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP). Select this option to block traffic between wireless clients in the BSS. Wireless clients can still access the wired network but cannot communicate with each other.
Security Mode	Select **WPA-PSK** or **WPA2-PSK** to add security on this wireless network. The wireless clients which want to associate to this network must have same wireless security settings as this device. After you select to use a security, additional options appears in this screen. Or you can select **No Security** to allow any client to associate this network without authentication. Note: If you do not enable any wireless security on your WAH7130, your network is accessible to any wireless networking device that is within range.
Encryption Type	Select the encryption protocol (**TKIP**, **AES-CCMP** or **Auto**) for data encryption. Select **AES-CCMP** if your wireless clients can all use AES-CCMP. Otherwise, select **TKIP** or select **Auto** to allow the wireless clients to use either TKIP or AES-CCMP.
Pre-Shared Key	**WPA-PSK** or **WPA2-PSK** uses a simple common password for authentication. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols). Type a pre-shared key less than 64 case-sensitive HEX characters ("0-9", "A-F").
Transmission (Tx) Power	Set the output power of the WAH7130. It is suggested that you select **Low** to decrease the output power of the WAH7130 to save battery power and reduce interference with nearby APs (if any).

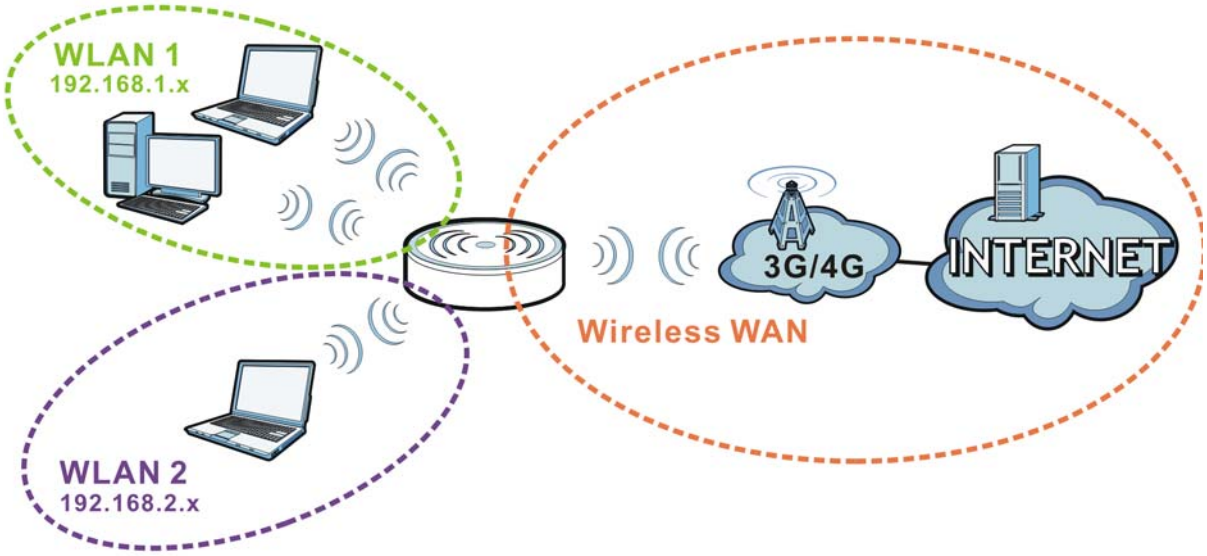
Table 19 Network > Wireless LAN > General (continued)

LABEL	DESCRIPTION
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

5.3 Guest Wi-Fi Screen

In addition to the default (first) wireless LAN (configured in the **Wireless LAN > General** screen), this screen allows you to enable and configure a second wireless LAN (guest Wi-Fi) on the WAH7130. The wireless clients associated with guest Wi-Fi will be on a different subnet (192.168.2.x) from the WAH7130's default wireless network.

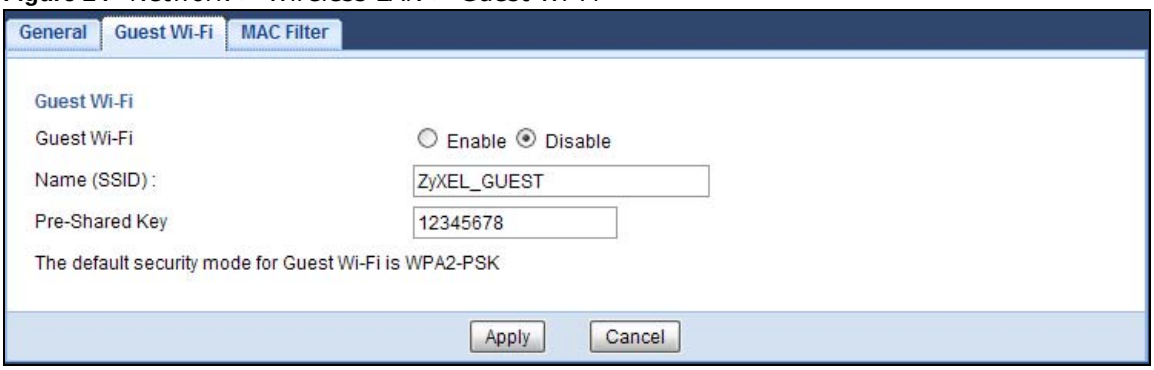
Figure 23 Default and Guest WLANs



This allows you to use one access point to provide two BSSs simultaneously. You can then assign varying security types to different SSIDs. Wireless clients can use different SSIDs to associate with the same access point.

Click **Network > Wireless LAN > Guest Wi-Fi**. The following screen displays.

Figure 24 Network > Wireless LAN > Guest Wi-Fi



The following table describes the labels in this screen.

Table 20 Network > Wireless LAN > Guest Wi-Fi

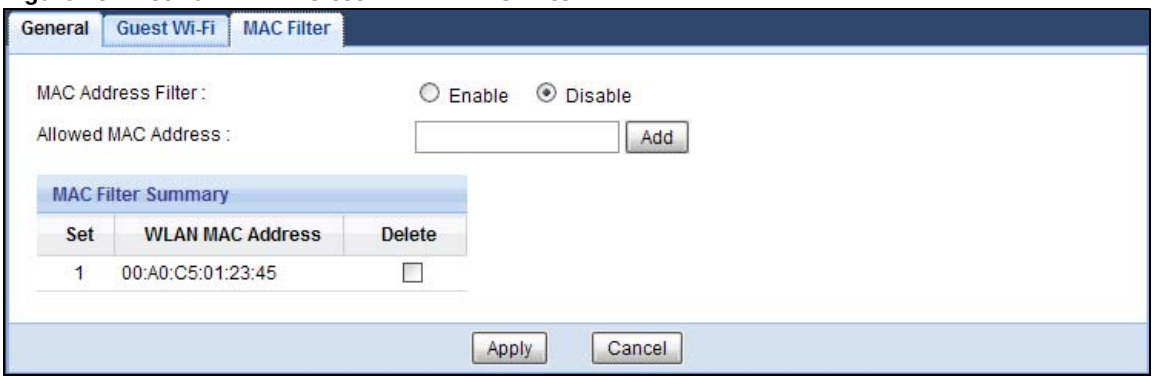
LABEL	DESCRIPTION
Guest Wi-Fi	Select **Enable** to turn on the guest wireless network on the WAH7130. Otherwise, select **Disable** to turn it off.
Name (SSID)	Enter a descriptive name for the guest wireless LAN using up to 32 printable characters.
Pre-Shared Key	The default security mode for guest Wi-Fi is WPA2-PSK. Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols) or type a pre-shared key less than 64 case-sensitive HEX characters ("0-9", "A-F") for data encryption.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

5.4 MAC Filter Screen

The MAC filter screen allows you to configure the WAH7130 to give exclusive access to devices (**Allow**) or exclude devices from accessing the WAH7130 (**Deny**). Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. You need to know the MAC address of the devices to configure this screen.

To change your WAH7130's MAC filter settings, click **Network** > **Wireless LAN** > **MAC Filter**. The screen appears as shown.

Figure 25 Network > Wireless LAN > MAC Filter



The following table describes the labels in this menu.

Table 21 Network > Wireless LAN > MAC Filter

LABEL	DESCRIPTION
MAC Address Filter	Select to turn on (**Enable**) or off (**Disable**) MAC address filtering.
Allowed MAC Address	Enter the MAC addresses (in XX:XX:XX:XX:XX:XX format) of the wireless client to be allowed access to the WAH7130. Click **Add** to create a new entry in the summary table.
MAC Filter Summary	
Set	This is the index number of the MAC address.

Table 21 Network > Wireless LAN > MAC Filter (continued)

LABEL	DESCRIPTION
WLAN MAC Address	This is the MAC address of the wireless client that are allowed access to the WAH7130.
Delete	Select an entry and click **Apply** to remove it from the summary table.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

6 LAN

6.1 Overview

This chapter describes how to configure LAN settings.

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building.

The LAN screen can help you configure a management IP address.

The WAH7130 has built-in DHCP server capability that assigns IP addresses to devices that support DHCP client capability.

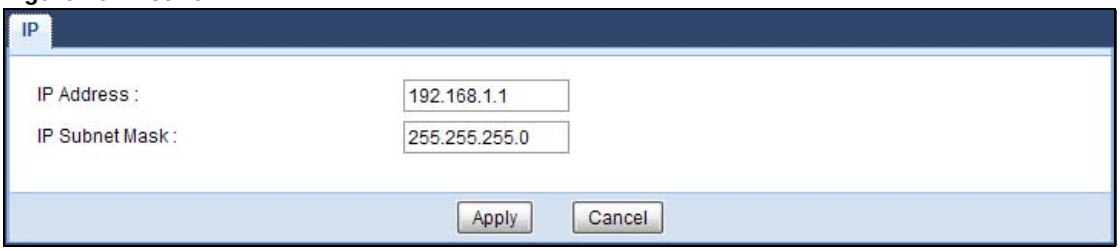
6.2 What You Can Do

- Use the **IP** screen to change the management IP address for your WAH7130 (Section 6.3 on page 49).

6.3 LAN IP Screen

Use this screen to change the IP address for your WAH7130. Click **Network > LAN > IP**.

Figure 26 Network > LAN > IP



The following table describes the labels in this screen.

Table 22 Network > LAN > IP

LABEL	DESCRIPTION
IP Address	Type the IP address of your WAH7130 in dotted decimal notation.

Table 22 Network > LAN > IP (continued)

LABEL	DESCRIPTION
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your WAH7130 will automatically calculate the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the WAH7130.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7

DHCP Server

7.1 Overview

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server. You can configure the WAH7130's LAN as a DHCP server or disable it. When configured as a server, the WAH7130 provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be manually configured.

7.1.1 What You Can Do

- Use the **General** screen to enable the DHCP server (Section 7.2 on page 51).
- Use the **Client List** screen to view the current DHCP client information (Section 7.3 on page 52).

7.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

IP Pool Setup

The WAH7130 is pre-configured with a pool of 150 IP addresses starting from 192.168.1.100 to 192.168.1.249. This configuration leaves 103 IP addresses (excluding the WAH7130 itself) in the lower range (192.168.1.2 to 192.168.1.99) and from 192.168.1.250 to 192.168.1.254 for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

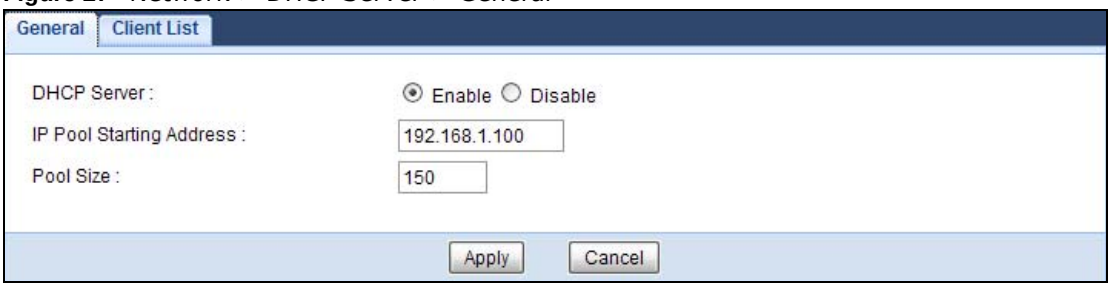
MAC Addresses

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02. Find out the MAC addresses of your network devices if you intend to add them to the **DHCP Server > Client List** screen.

7.2 DHCP Server General Screen

Use this screen to enable the DHCP server. Click **Network** > **DHCP Server**. The following screen displays.

Figure 27 Network > DHCP Server > General



The following table describes the labels in this screen.

Table 23 Network > DHCP Server > General

LABEL	DESCRIPTION
DHCP Server	Select **Enable** to activate DHCP for LAN. DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (computers) to obtain TCP/IP configuration at startup from a server. Enable the DHCP server unless your ISP instructs you to do otherwise. Select **Disable** to stop the WAH7130 acting as a DHCP server. When configured as a server, the WAH7130 provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computers must be manually configured. When set as a server, fill in the following four fields.
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool for LAN.
Pool Size	This field specifies the size, or count of the IP address pool for LAN.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to begin configuring this screen afresh.

7.3 DHCP Client List Screen

The DHCP table shows current DHCP client information (including IP Address, Host Name and MAC Address) of network clients using the WAH7130's DHCP servers.

Configure this screen to always assign an IP address to a MAC address (and host name). Click **Network > DHCP Server > Client List**.

Note: You can also view a read-only client list by clicking **Monitor > DHCP Table**.

Figure 28 Network > DHCP Server > Client List

The following table describes the labels in this screen.

Table 24 Network > DHCP Server > Client List

LABEL	DESCRIPTION
#	This is the index number of the host computer.
Status	This field displays whether the connection to the host computer is up (a yellow bulb) or down (a gray bulb).
Host Name	This field displays the computer host name.
IP Address	This field displays the IP address relative to the # field listed above.
MAC Address	This field shows the MAC address of the computer with the name in the **Host Name** field. Every Ethernet device has a unique MAC (Media Access Control) address which uniquely identifies a device. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Reserve	Select this if you want to reserve the IP address for this specific MAC address.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to reload the previous configuration for this screen.

8 NAT

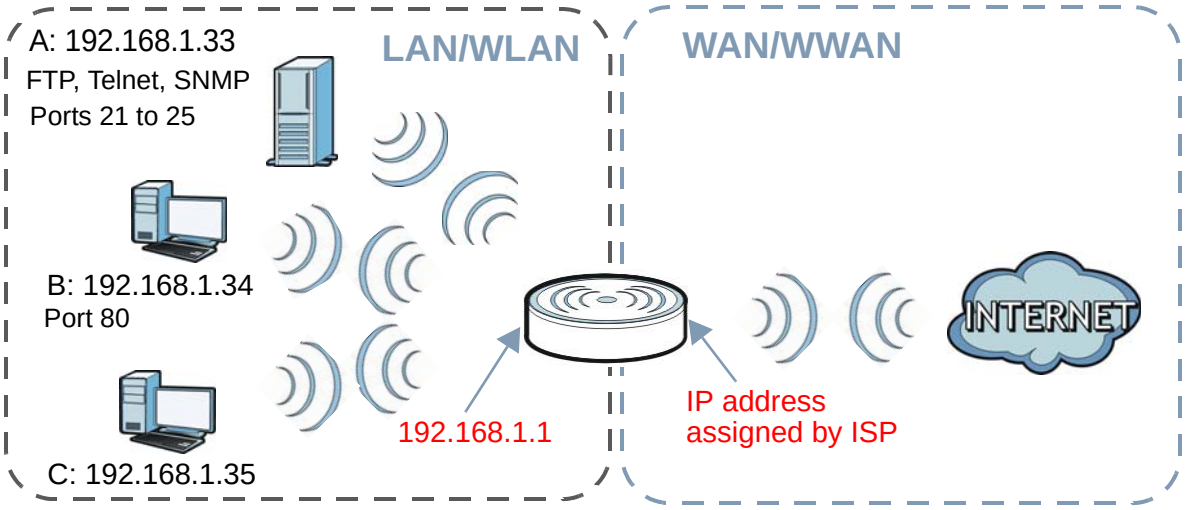
8.1 Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

The figure below is a simple illustration of a NAT network. You want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example).

You assign the LAN IP addresses to the devices (**A** to **C**) connected to your WAH7130. The ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet. All traffic coming from **A** to **C** going out to the Internet use the IP address of the WAH7130, which is 192.168.1.1.

Figure 29 NAT Example



This chapter discusses how to configure NAT on the WAH7130.

8.1.1 What You Can Do

- Use the **General** screen to view the NAT status (Section 8.2 on page 57).
- Use the **Port Forwarding** screen to set a default server and change your WAH7130's port forwarding settings to forward incoming service requests to the server(s) on your local network (Section 8.3 on page 57).

8.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

Inside/Outside

This denotes where a host is located relative to the WAH7130, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/Local

This denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note: Inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet.

An inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 25 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

Note: NAT never changes the IP address (either local or global) of an outside host.

What NAT Does

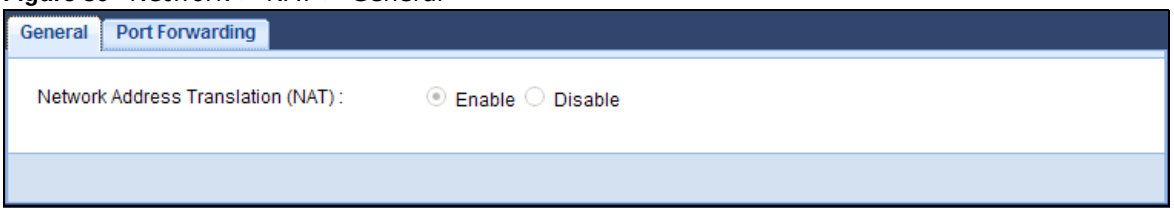
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your WAH7130 filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to *RFC 1631*, *The IP Network Address Translator (NAT)*.

8.2 General

Use this read-only screen to view the NAT status. Click **Network > NAT** to open the **General** screen.

Figure 30 Network > NAT > General



The following table describes the labels in this screen.

Table 26 Network > NAT > General

LABEL	DESCRIPTION
Network Address Translation (NAT)	Network Address Translation (NAT) allows the translation of an Internet protocol address used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). NAT is always enabled on the WAH7130.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.3 Port Forwarding Screen

Use this screen to forward incoming service requests to the server(s) on your local network and set a default server. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

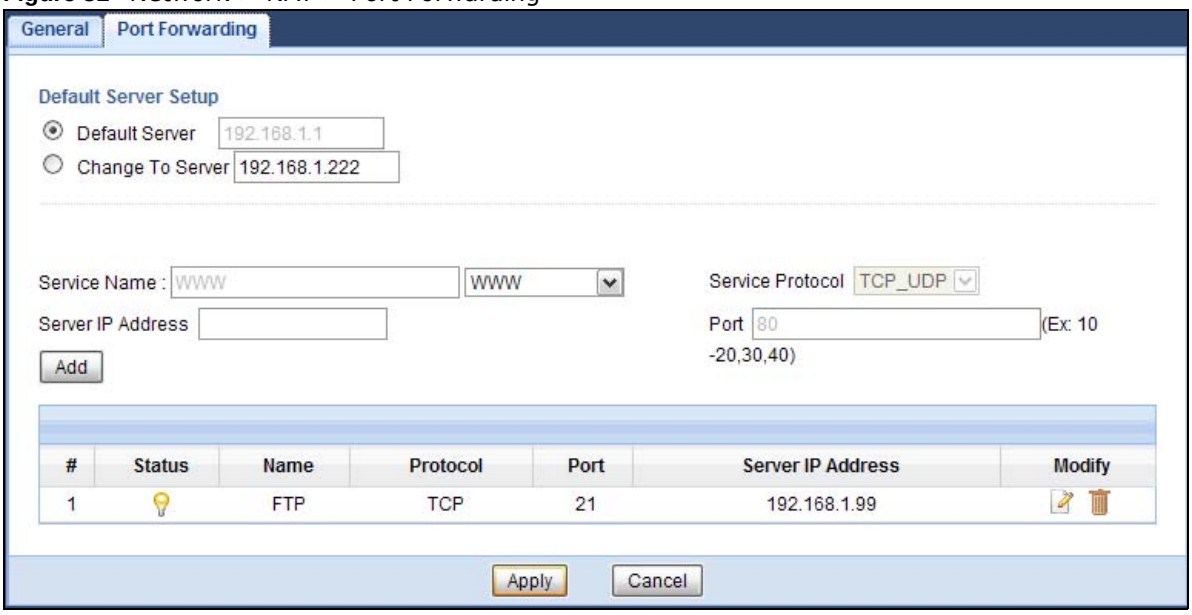
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Port forwarding allows you to define the local servers to which the incoming services will be forwarded. To change your WAH7130's port forwarding settings, click **Network > NAT** > **Port Forwarding**. The screen appears as shown.

Note: If you do not assign a **Default Server**, the WAH7130 discards all packets received for ports that are not specified in this screen or remote management.

Figure 31 Network > NAT > Port Forwarding



The following table describes the labels in this screen.

Table 27 Network > NAT > Port Forwarding

LABEL	DESCRIPTION
Default Server Setup	
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in the **Port Forwarding** screen. You can decide whether you want to use the default server or specify a server manually. Select this to use the default server.
Change to Server	Select this and manually enter the server's IP address.
Service Name	Select a pre-defined service from the drop-down list box. The pre-defined service port number(s) and protocol will be displayed in the port forwarding summary table. Otherwise, select **User define** to manually enter the port number(s) and select the IP protocol.
Service Protocol	Select the transport layer protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP_UDP**. If you have chosen a pre-defined service in the **Service Name** field, the protocol will be configured automatically.
Server IP Address	Enter the inside IP address of the virtual server here and click **Add** to add it in the port forwarding summary table.
Port	Enter the service port number(s). If you have chosen a pre-defined service in the **Service Name** field, the port number will be configured automatically.
#	This is the number of an individual port forwarding server entry.
Status	This icon is turned on when the rule is enabled.
Name	This field displays a name to identify this rule.
Protocol	This is the transport layer protocol used for the service.
Port	This field displays the port number(s) that identifies a service.
Server IP Address	This field displays the inside IP address of the server.

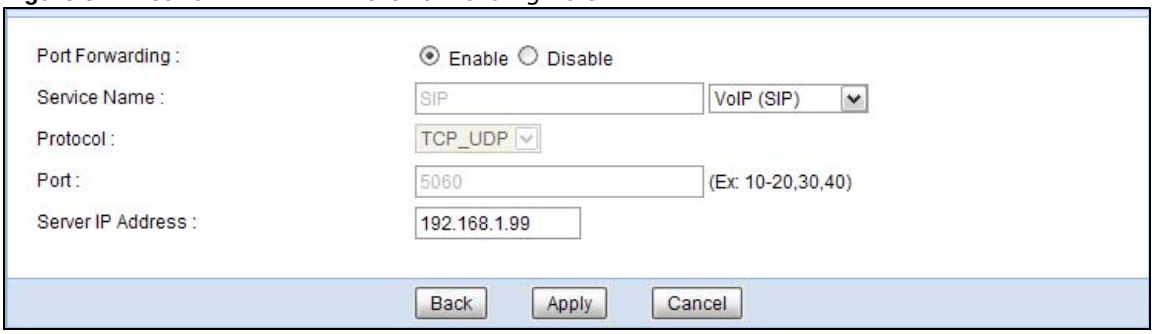
Table 27 Network > NAT > Port Forwarding (continued)

LABEL	DESCRIPTION
Modify	Click the **Edit** icon to open the edit screen where you can modify an existing rule. Click the **Delete** icon to remove a rule.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.3.1 Port Forwarding Edit Screen

This screen lets you edit a port forwarding rule. Click a rule's **Edit** icon in the **Port Forwarding** screen to open the following screen.

Figure 32 Network > NAT > Port Forwarding Edit



The following table describes the labels in this screen.

Table 28 Network > NAT > Port Forwarding Edit

LABEL	DESCRIPTION
Port Forwarding	Select **Enable** to turn on this rule and the requested service can be forwarded to the host with a specified internal IP address. Select **Disable** to disallow forwarding of these ports to an inside server without having to delete the entry.
Service Name	Type a name (of up to 31 printable characters) to identify this rule in the first field next to **Service Name**. Otherwise, select a predefined service in the second field next to **Service Name**. The predefined service name and port number(s) will display in the **Service Name** and **Port** fields.
Protocol	Select the transport layer protocol supported by this virtual server. Choices are **TCP**, **UDP**, or **TCP_UDP**. If you have chosen a pre-defined service in the **Service Name** field, the protocol will be configured automatically.
Port	Type a port number(s) to define the service to be forwarded to the specified server. To specify a range of ports, enter a hyphen (-) between the first port and the last port, such as 10-.
Server IP Address	Type the IP address of the server on your LAN that receives packets from the port(s) specified in the **Port** field.
Back	Click **Back** to return to the previous screen.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to begin configuring this screen afresh.

8.4 Technical Reference

The following section contains additional technical information about the WAH7130 features described in this chapter.

8.4.1 NAT Port Forwarding: Services and Port Numbers

A port forwarding set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make accessible to the outside world even though NAT makes your whole inside network appear as a single machine to the outside world.

Use the **Port Forwarding** screen to forward incoming service requests to the server(s) on your local network. You may enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example both FTP and web service), it might be better to specify a range of port numbers.

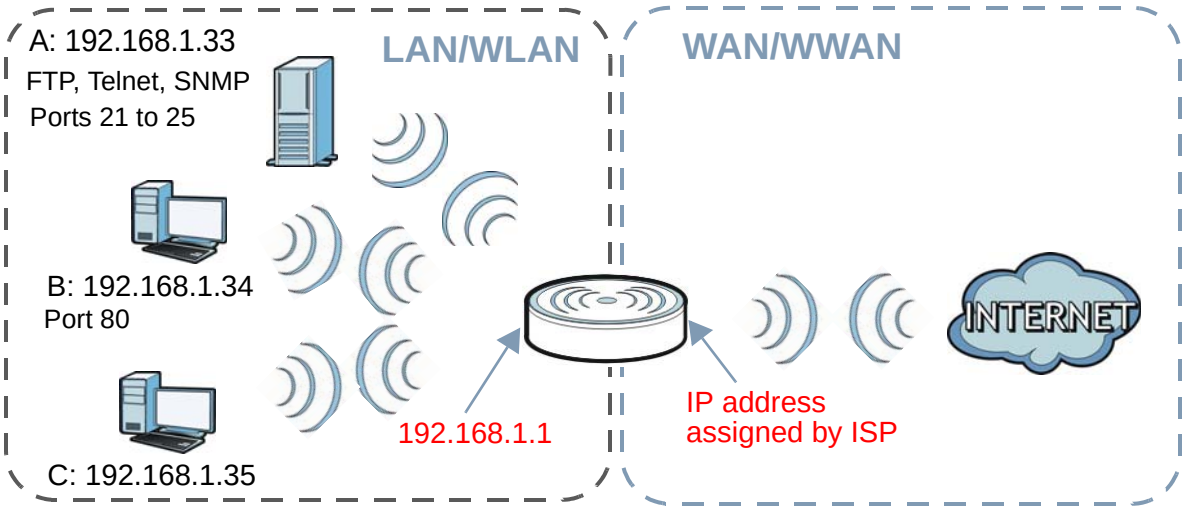
In addition to the servers for specified services, NAT supports a default server. A service request that does not have a server explicitly designated for it is forwarded to the default server. If the default is not defined, the service request is simply discarded.

Note: Many residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

8.4.2 NAT Port Forwarding Example

Let's say you want to assign ports 21-25 to one FTP, Telnet and SMTP server (**A** in the example), port 80 to another (**B** in the example) and assign a default server IP address of 192.168.1.35 to a third (**C** in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Figure 33 Multiple Servers Behind NAT Example



9

Firewall

9.1 Overview

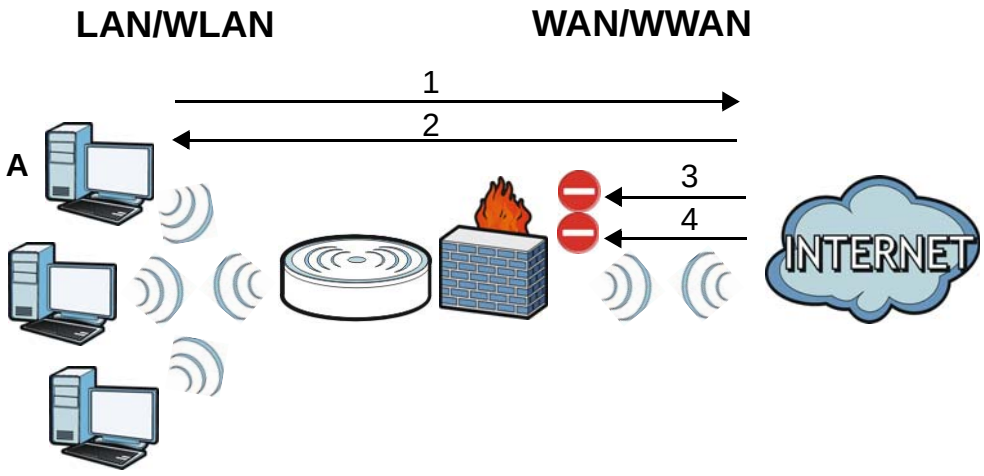
Use these screens to enable and configure the firewall that protects your WAH7130 and your LAN from unwanted or malicious traffic.

Enable the firewall to protect your LAN computers from attacks by hackers on the Internet and control access between the LAN/WLAN and WAN/WWAN. By default the firewall:

- allows traffic that originates from your LAN/WLAN computers to go to all of the networks.
- blocks traffic that originates on the other networks from going to the LAN/WLAN.

The following figure illustrates the default firewall action. User **A** can initiate an IM (Instant Messaging) session from the LAN/WLAN to the WAN/WWAN (1). Return traffic for this session is also allowed (2). However other traffic initiated from the WAN/WWAN is blocked (3 and 4).

Figure 34 Default Firewall Action



9.1.1 What You Can Do

- Use the **General** screen to enable or disable the WAH7130's firewall (Section 9.2 on page 65).
- Use the **Service Blocking** screen to enable service blocking. You can enter/delete/modify the services you want to block and the date/time you want to block them (Section 9.3 on page 65).

9.1.2 What You Need To Know

The following terms and concepts may help as you read through this chapter.

What is a Firewall?

Originally, the term “firewall” referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term "firewall" is a system or group of systems that enforces an access-control policy between two networks. It may also be defined as a mechanism used to protect a trusted network from a network that is not trusted.

Guidelines For Enhancing Security With Your Firewall

1 Change the default password via Web Configurator.

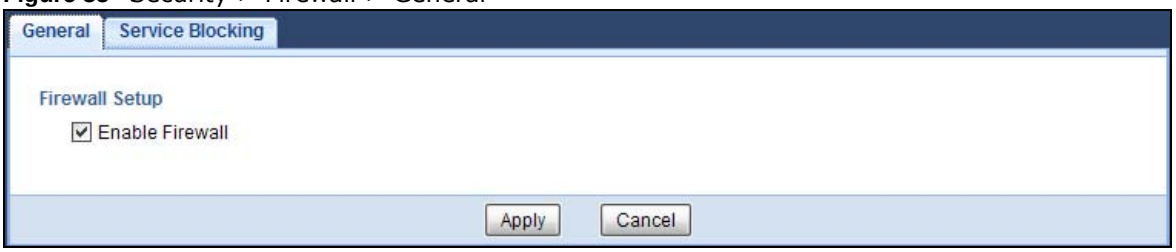
2 Don't enable any local service (such as NTP) that you don't use. Any enabled service could present a potential security risk. A determined hacker might be able to find creative ways to misuse the enabled services to access the firewall or the network.

3 Keep the firewall in a secured (locked) room.

9.2 General Screen

Use this screen to enable or disable the WAH7130’s firewall. Click **Security** > **Firewall** to open the **General** screen.

Figure 35 Security > Firewall > General



The following table describes the labels in this screen.

Table 29 Security > Firewall > General

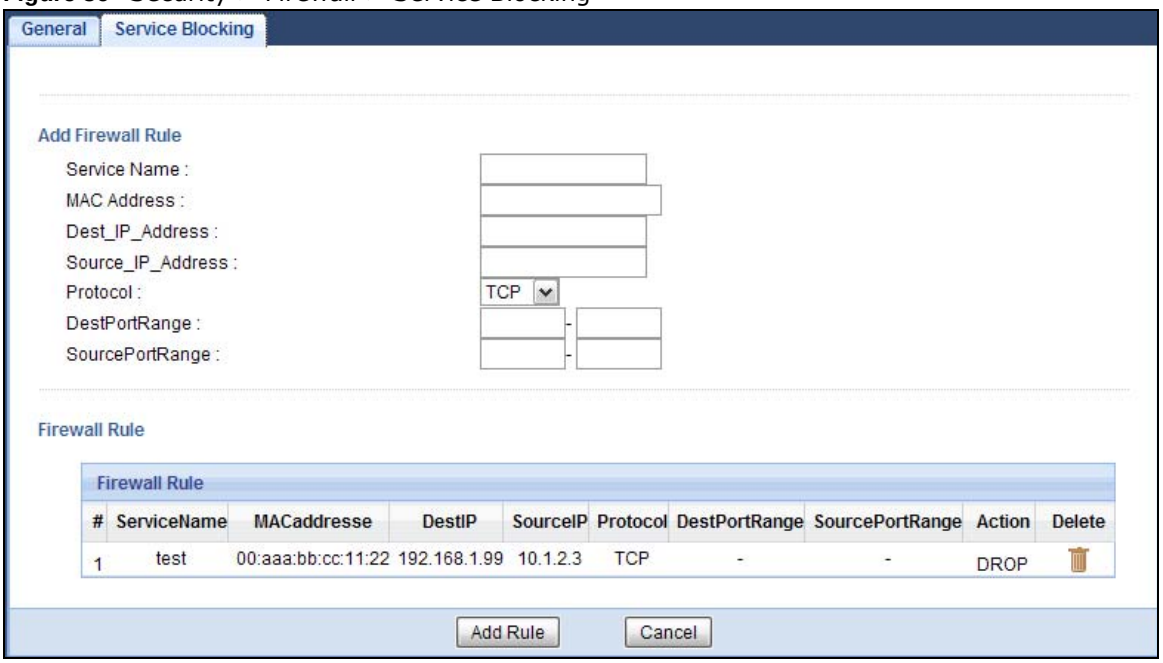
LABEL	DESCRIPTION
Enable Firewall	Select this check box to activate the firewall. The WAH7130 performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated.
Apply	Click **Apply** to save the settings.
Cancel	Click **Cancel** to start configuring this screen again.

9.3 Service Blocking Screen

You can use this screen to enable service blocking, enter/delete/modify the services you want to block and the date/time you want to block them.

Click **Security** > **Firewall** > **Service Blocking**. The screen appears as shown next.

Figure 36 Security > Firewall > Service Blocking



The following table describes the labels in this screen.

Table 30 Security > Firewall > Service Blocking

LABEL	DESCRIPTION
Add Firewall Rule	
Service Name	Enter a name that identifies or describes the firewall rule.
MAC Address	Enter the MAC address of the computer for which the firewall rule applies.
Dest IP Address	Enter the IP address of the computer to which traffic for the application or service is entering. The WAH7130 applies the firewall rule to traffic initiating from this computer.
Source IP Address	Enter the IP address of the computer that initializes traffic for the application or service. The WAH7130 applies the firewall rule to traffic initiating from this computer.
Protocol	Select the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	Enter the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	Enter the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Add Rule	Click **Add** to save the firewall rule.
Firewall Rule	
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn.
Service Name	This is a name that identifies or describes the firewall rule.
MAC Address	This is the MAC address of the computer for which the firewall rule applies.
Dest IP	This is the IP address of the computer to which traffic for the application or service is entering.
Source IP	This is the IP address of the computer from which traffic for the application or service is initialized.

Table 30 Security > Firewall > Service Blocking (continued)

LABEL	DESCRIPTION
Protocol	This is the protocol (**TCP**, **UDP** or **ICMP**) used to transport the packets for which you want to apply the firewall rule.
Dest Port Range	This is the port number/range of the destination that define the traffic type, for example TCP port 80 defines web traffic.
Source Port Range	This is the port number/range of the source that define the traffic type, for example TCP port 80 defines web traffic.
Action	**DROP** - Traffic matching the conditions of the firewall rule are stopped.
Delete	Click **Delete** to remove the firewall rule.
Cancel	Click **Cancel** to start configuring this screen again.

See Appendix A on page 83 for commonly used services and port numbers.

10 Maintenance

10.1 Overview

This chapter provides information on the **Maintenance** screens.

10.2 What You Can Do

- Use the **General** screen to set the timeout period of the management session (Section 10.3 on page 69).
- Use the **Password** screen to change your WAH7130's system password (Section 10.4 on page 70).
- Use the **Time** screen to change your WAH7130's time and date (Section 10.5 on page 71).
- Use the **Firmware Upgrade** screen to upload firmware to your WAH7130 (Section 10.6 on page 72).
- Use the **Backup / Restore** screen to view information related to factory defaults, backup configuration, and restoring configuration (Section 10.8 on page 75).
- Use the **Restart** screen to reboot the WAH7130 without turning the power off (Section 10.8 on page 75).
- Use the **Language** screen to change the language for the Web Configurator (Section 10.9 on page 75).

10.3 General Screen

Use this screen to set the management session timeout period. Click **Maintenance** > **General**. The following screen displays.

Figure 37 Maintenance > General

The following table describes the labels in this screen.

Table 31 Maintenance > General

LABEL	DESCRIPTION
System Name	System Name is a unique name to identify the WAH7130 in an Ethernet network.
Domain Name	Enter the domain name you want to give to the WAH7130.
Administrator Inactivity Timer	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to begin configuring this screen afresh.

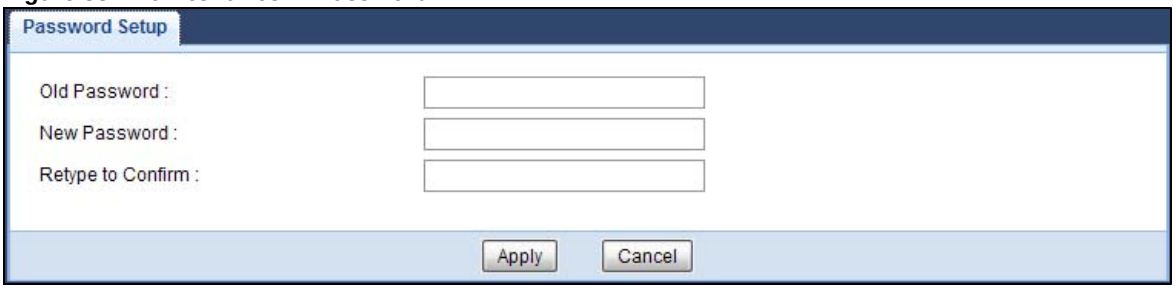
10.4 Password Screen

It is strongly recommended that you change your WAH7130's password.

If you forget your WAH7130's password (or IP address), you will need to reset the device. See Section 10.8 on page 75 for details.

Click **Maintenance** > **Password**. The screen appears as shown.

Figure 38 Maintenance > Password



The following table describes the labels in this screen.

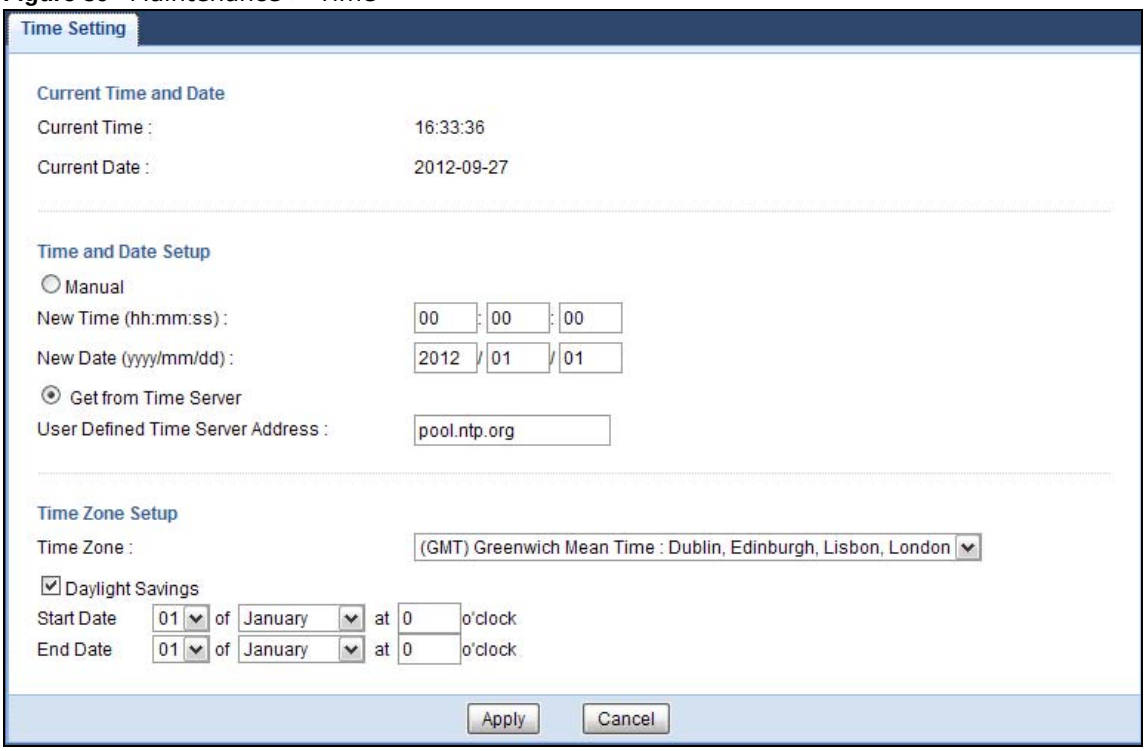
Table 32 Maintenance > Password

LABEL	DESCRIPTION
Old Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type your new system password (up to 30 characters). Note that as you type a password, the screen displays an asterisk (*) for each character you type.
Retype to Confirm	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.5 Time Setting Screen

Use this screen to configure the WAH7130's time based on your local time zone. To change your WAH7130's time and date, click **Maintenance** > **Time**. The screen appears as shown.

Figure 39 Maintenance > Time



The following table describes the labels in this screen.

Table 33 Maintenance > Time

LABEL	DESCRIPTION
Current Time and Date	
Current Time	This field displays the time of your WAH7130. Each time you reload this page, the WAH7130 synchronizes the time with the time server.
Current Date	This field displays the date of your WAH7130. Each time you reload this page, the WAH7130 synchronizes the date with the time server.
Current Time and Date	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, Time Zone and Daylight Saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. When you select **Manual**, enter the new time in this field and then click **Apply**.

Table 33 Maintenance > Time (continued)

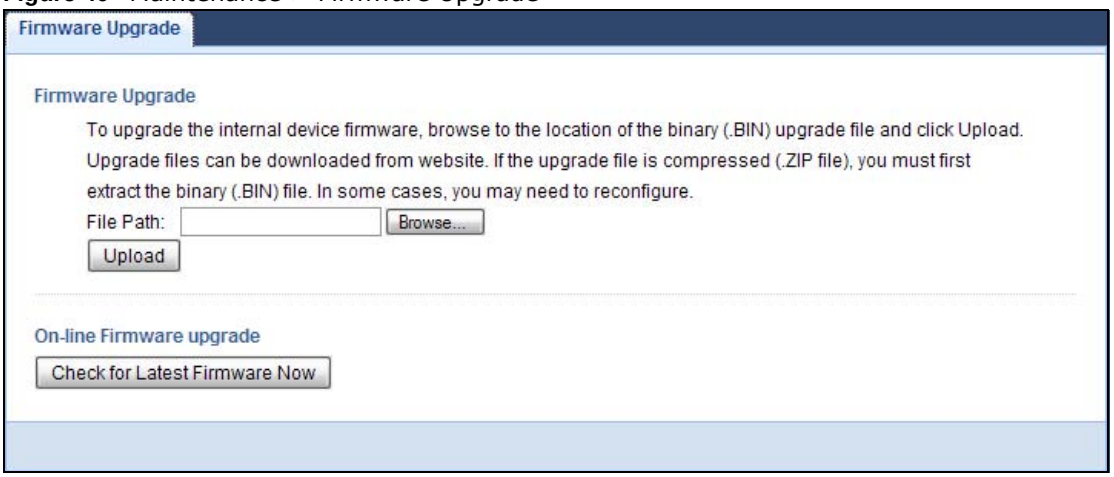
LABEL	DESCRIPTION
New Date (yyyy/mm/dd)	This field displays the last updated date from the time server or the last date configured manually. When you select **Manual**, enter the new date in this field and then click **Apply**.
Get from Time Server	Select this radio button to have the WAH7130 get the time and date from the time server you specified below.
User Defined Time Server Address	Select **User Defined Time Server Address** and enter the IP address or URL (up to 20 extended ASCII characters in length) of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Daylight Savings	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **11**, **March** and type **2** in the **o'clock** field for the year 2012. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **25**, **March** for the year 2012. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected **Daylight Savings**. The **o'clock** field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select **4**, **November** and type 2 in the **o'clock** field for the year 2012. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select **28**, **October** for the year 2012. The time you type in the **o'clock** field depends on your time zone. In Germany for instance, you would type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click **Apply** to save your changes back to the WAH7130.
Cancel	Click **Cancel** to begin configuring this screen afresh.

10.6 Firmware Upgrade Screen

Find firmware at www.zyxel.com in a file that uses the version number and project code with a "*.bin" extension, for example, "V1.00(AAGY.0).bin". The upload process uses HTTP (Hypertext Transfer Protocol) and may take up to two minutes. After a successful upload, the system will reboot.

Click **Maintenance > Firmware Upgrade**. Follow the instructions in this screen to upload firmware to your WAH7130.

Figure 40 Maintenance > Firmware Upgrade


Firmware Upgrade
Firmware Upgrade
To upgrade the internal device firmware, browse to the location of the binary (.BIN) upgrade file and click Upload.
Upgrade files can be downloaded from website. If the upgrade file is compressed (.ZIP file), you must first
extract the binary (.BIN) file. In some cases, you may need to reconfigure.
File Path:
Browse...
Upload
On-line Firmware upgrade
Check for Latest Firmware Now

The following table describes the labels in this screen.

Table 34 Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click **Upload** to begin the upload process. This process may take up to two minutes.
Check for Latest Firmware Now	Click this to check for the latest updated firmware.

Note: Do not turn off the WAH7130 while firmware upload is in progress!

Wait two minutes before logging into the WAH7130 again. The WAH7130 automatically restarts in this time causing a temporary network disconnect. After two minutes, log in again and check your new firmware version in the **Status** screen.

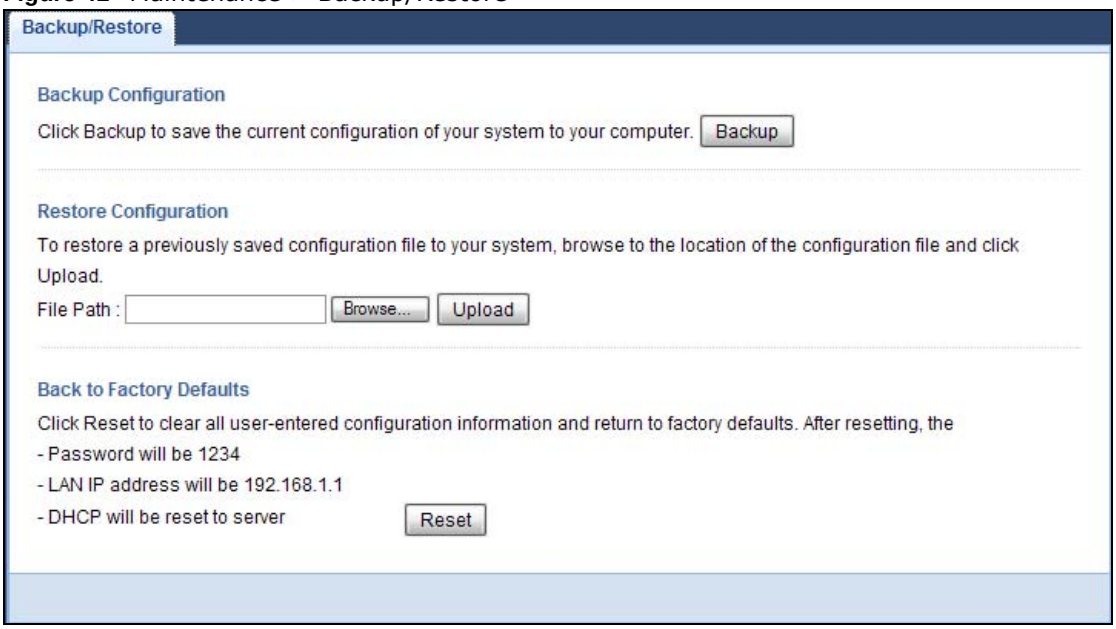
10.7 Configuration Backup/Restore Screen

Backup configuration allows you to back up (save) the WAH7130's current configuration to a file on your computer. Once your WAH7130 is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

Restore configuration allows you to upload a new or previously saved configuration file from your computer to your WAH7130.

Click **Maintenance > Backup/Restore**. Information related to factory defaults, backup configuration, and restoring configuration appears as shown next.

Figure 41 Maintenance > Backup/Restore


Backup/Restore
Backup Configuration
Click Backup to save the current configuration of your system to your computer.
Backup
Restore Configuration
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.
File Path :
Browse...
Upload
Back to Factory Defaults
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the
- Password will be 1234
- LAN IP address will be 192.168.1.1
- DHCP will be reset to server
Reset

The following table describes the labels in this screen.

Table 35 Maintenance > Backup/Restore

LABEL	DESCRIPTION
Backup	Click **Backup** to save the WAH7130's current configuration to your computer.
File Path	Type in the location of the file you want to upload in this field or click **Browse...** to find it.
Browse...	Click **Browse...** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click **Upload** to begin the upload process. Note: Do not turn off the WAH7130 while configuration file upload is in progress. After you see a "configuration upload successful" screen, you must then wait one minute before logging into the WAH7130 again. The WAH7130 automatically restarts in this time causing a temporary network disconnect. If you see an error screen, click Back to return to the Backup/Restore screen.
Reset	Pressing the **Reset** button in this section clears all user-entered configuration information and returns the WAH7130 to its factory defaults. You can also press the **RESET** button on the rear panel to reset the factory defaults of your WAH7130. Refer to the chapter about introducing the Web Configurator for more information on the **RESET** button.

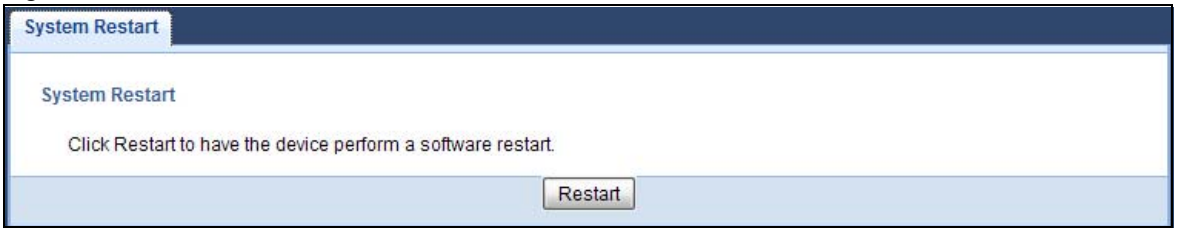
Note: If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default WAH7130 IP address (192.168.1.1).

10.8 Restart Screen

System restart allows you to reboot the WAH7130 without turning the power off.

Click **Maintenance > Restart** to open the following screen.

Figure 42 Maintenance > Restart



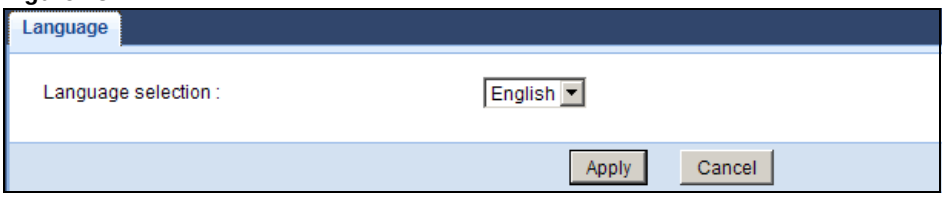
Click **Restart** to have the WAH7130 reboot. This does not affect the WAH7130's configuration.

10.9 Language Screen

Use this screen to change the language for the Web Configurator.

Select the language you prefer and click **Apply**. The Web Configurator language changes after a while without restarting the WAH7130.

Figure 43



11

Troubleshooting

11.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- WAH7130 Access and Login
- Internet Access
- Wireless LAN Connections

11.2 Power, Hardware Connections, and LEDs

The WAH7130's OLED display is not on or the LED is off.

1. Make sure the battery does not run out.
2. The WAH7130 may go into sleep mode or the OLED display is disabled. See Section 1.6 on page 13 for how to wake up the WAH7130 and/or turn on the OLED display.
3. If the problem continues, contact the vendor.

The LED does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.7 on page 15.
2. Check the hardware installation. See the Quick Start Guide.
3. The WAH7130 may go into sleep mode or the OLED display is disabled. See Section 1.6 on page 13 for how to wake up the WAH7130 and/or turn on the OLED display.
4. If the problem continues, contact the vendor.

11.3 WAH7130 Access and Login

I don't know the IP address of my WAH7130.

1. The default management IP address of the WAH7130 is **192.168.1.1**.
2. If you changed the IP address and have forgotten it, you might get the IP address of the WAH7130 by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the WAH7130 (it depends on the network), so enter this IP address in your Internet browser.
3. Reset your WAH7130 to change all settings back to their default. This means your current settings are lost. See Section 1.5 on page 12 in the **Troubleshooting** for information on resetting your WAH7130.

I forgot the password.

1. The default password is **1234**.
2. If this does not work, you have to reset the device to its factory defaults. See Section 1.5 on page 12.

I cannot see or access the **Login** screen in the Web Configurator.

1. Make sure you are using the correct IP address.
   - The default management IP address of the WAH7130 is **192.168.1.1**.
   - If you changed the IP address (Section 6.3 on page 49), use the new IP address.
   - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I don't know the IP address of my WAH7130.
2. Make sure the WAH7130 is turned on and the LED is behaving as expected. See the Quick Start Guide.
3. Make sure your computer is wirelessly connected to the WAH7130 and is in the same subnet as the WAH7130. See the troubleshooting suggestions for Wireless LAN Connections.
4. Make sure your Internet browser does not block pop-up windows and has JavaScript and Java enabled. See Appendix B on page 87.
5. Reset the WAH7130 to its factory defaults, and try to access the WAH7130 with the default IP address. See Section 1.5 on page 12.

6 If the problem continues, contact the vendor.

I can see the **Login** screen, but I cannot log in to the WAH7130.

1 Make sure you have entered the password correctly. The default password is **1234**. This field is case-sensitive, so make sure [Caps Lock] is not on.

2 This can happen when you fail to log out properly from your last session. Try logging in again after 5 minutes.

3 Turn off and turn on the WAH7130 to restart it.

4 If this does not work, you have to reset the device to its factory defaults. See Section 1.5 on page 12.

11.4 Internet Access

I cannot access the Internet.

1 Make sure the LED is behaving as expected. See the Quick Start Guide.

2 Make sure your mobile access information (such as APN) is entered correctly in the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 Make sure the WAH7130 is working in normal mode. See Section 1.6 on page 13 for how to wake up the WAH7130.

4 Make sure your SIM card's account is valid and has an active data plan. Check your service contract or contact your service provider directly.

5 Make sure your computer or wireless device is successfully connected to the WAH7130 via Wi-Fi. See the troubleshooting suggestions for Wireless LAN Connections.

6 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the WAH7130), but my Internet connection is not available anymore.

1 Make sure the LED is behaving as expected. See the Quick Start Guide and Section 1.7 on page 15.

2 Reboot the WAH7130.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LED, and check Section 1.7 on page 15. If the WAH7130 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 Check the signal strength. If the signal strength is low, try moving the WAH7130 closer to the ISP's base station if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3 Reboot the WAH7130.

4 If the problem continues, contact the network administrator or vendor.

11.5 Wireless LAN Connections

I cannot access the WAH7130 or ping any computer from the WLAN.

1 The WAH7130 may go into sleep mode. See Section 1.6 on page 13 for how to wake up the WAH7130.

2 Make sure the wireless adapter installed on your computer is working properly. Disable and re-enable it.

3 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard (802.11 mode) as the WAH7130.

4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the WAH7130 and also in the same subnet as the WAH7130.

5 Check that both the WAH7130 and the wireless adapter installed on your computer are using the same wireless and wireless security settings.

6 Make sure traffic from your computer is not blocked by the WAH7130's firewall service blocking.

What factors may cause intermittent or unstabled wireless LAN connection? How can I solve this problem?

The following factors may cause interference:

- Obstacles: walls, ceilings, furniture, and so on.

- Building Materials: metal doors, aluminum studs.
- Electrical devices: microwaves, monitors, electric motors, cordless phones, and other wireless devices.

To optimize the speed and quality of your wireless LAN connection, you can:

- Move your wireless device closer to the WAH7130 if the signal strength is low.
- Reduce wireless interference that may be caused by other wireless networks or surrounding wireless electronics such as cordless phones.
- Place the WAH7130where there are minimum obstacles (such as walls and ceilings) between the WAH7130 and the wireless client.
- Reduce the number of wireless clients connecting to the WAH7130 simultaneously.
- Try closing some programs that use the Internet, especially peer-to-peer applications. If the wireless client is sending or receiving a lot of information, it may have too many programs open that use the Internet.

A

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is user-defined, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is user-defined, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 36 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.

Table 36 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.

Table 36 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

B

Pop-up Windows, JavaScript and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: The screens used below belong to Internet Explorer version 6, 7 and 8. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

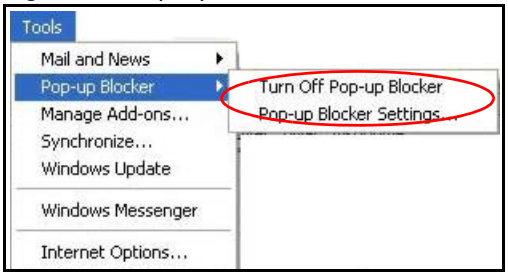
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 45 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 46 Internet Options: Privacy

3 Click **Apply** to save this setting.

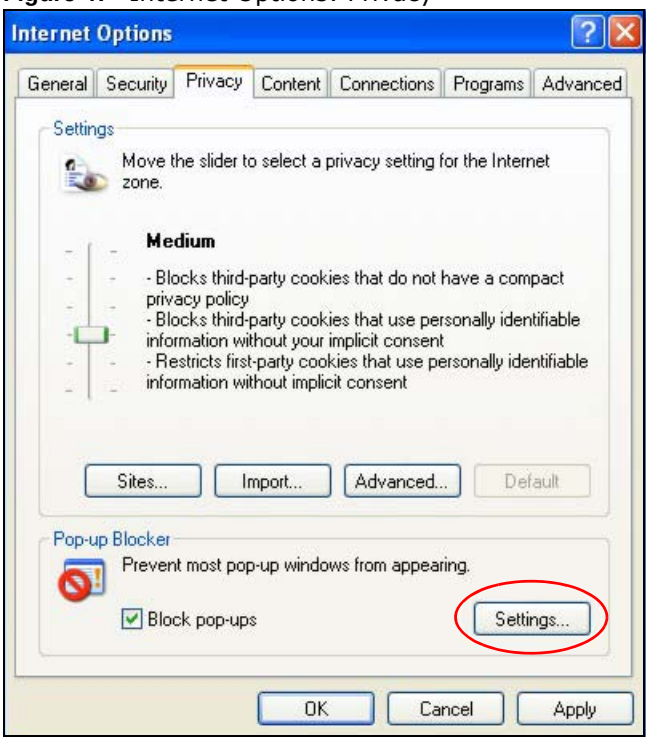
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...** to open the **Pop-up Blocker Settings** screen.

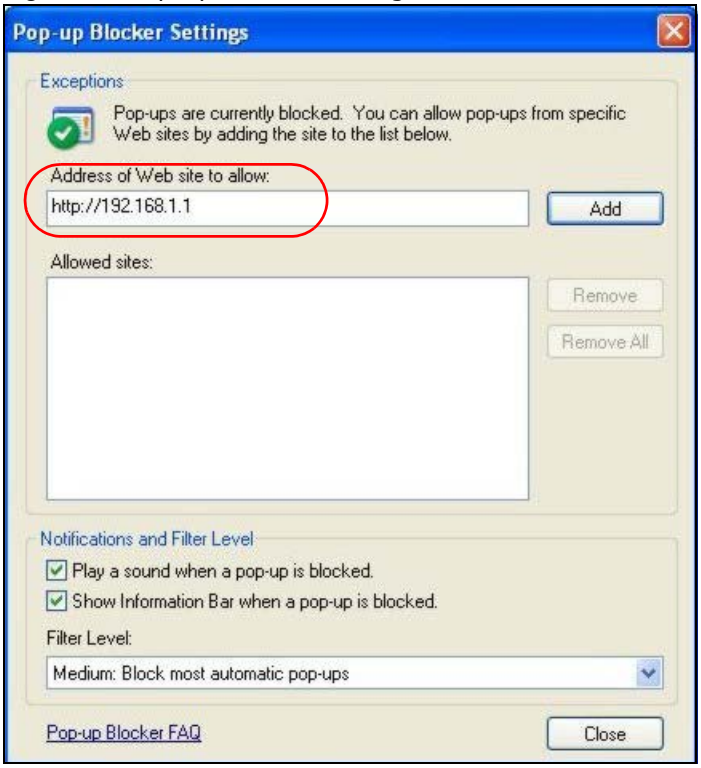
Figure 47 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix "http://". For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 48 Pop-up Blocker Settings


Pop-up Blocker Settings
Exceptions
Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.
Address of Web site to allow:
http://192.168.1.1
Add
Allowed sites:
Remove
Remove All
Notifications and Filter Level
Play a sound when a pop-up is blocked.
Show Information Bar when a pop-up is blocked.
Filter Level:
Medium: Block most automatic pop-ups
Pop-up Blocker FAQ
Close

5 Click **Close** to return to the **Privacy** screen.

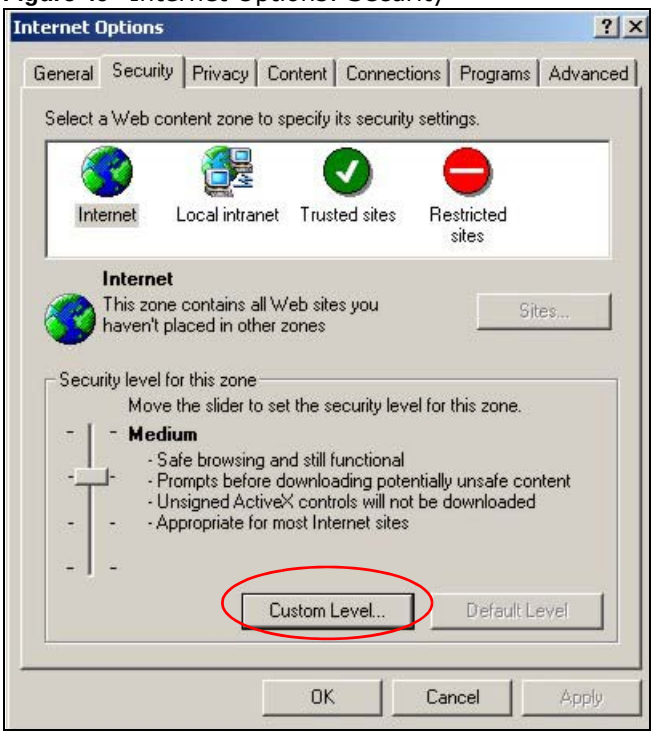
6 Click **Apply** to save this setting.

JavaScript

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScript are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 49 Internet Options: Security



2 Click the **Custom Level...** button.

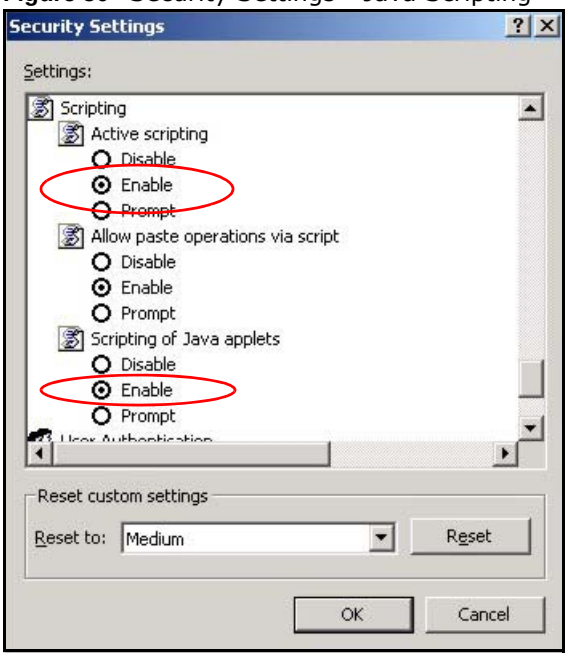
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 50 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

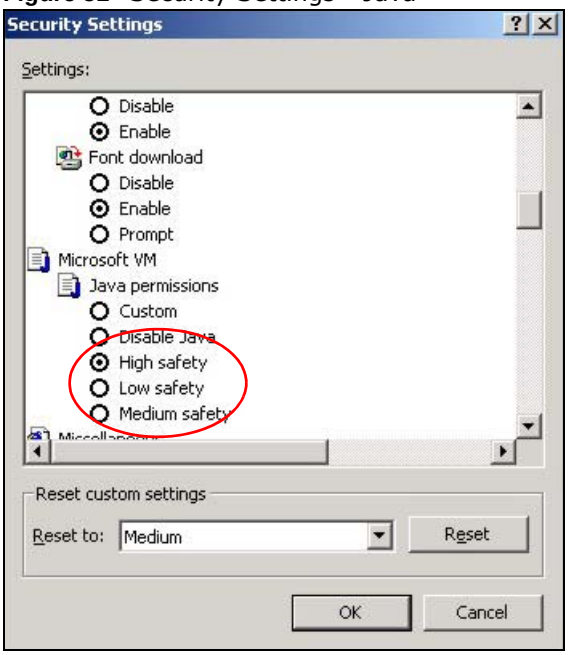
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 51 Security Settings - Java



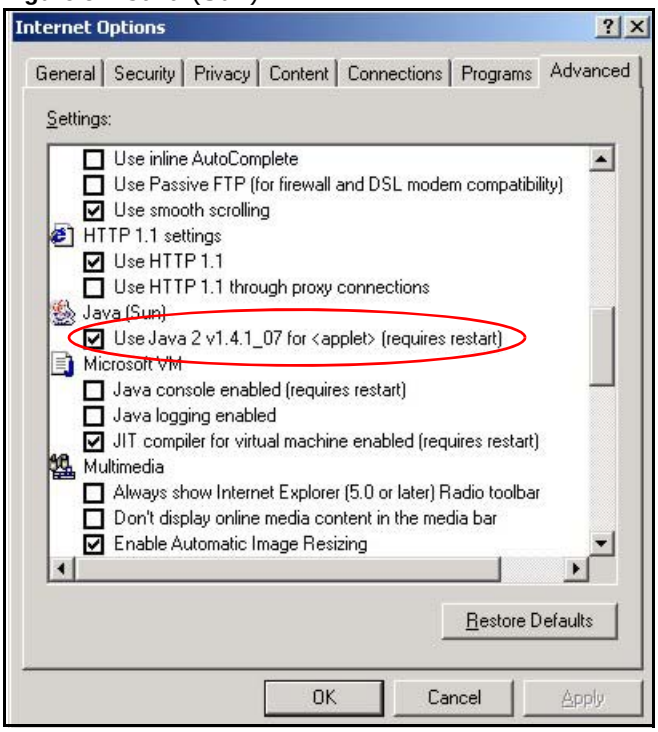
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 52 Java (Sun)

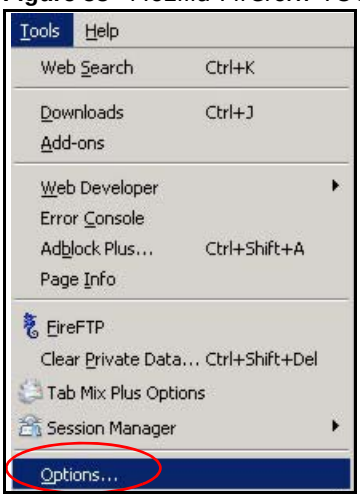


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary slightly. The steps below apply to Mozilla Firefox 3.0 as well.

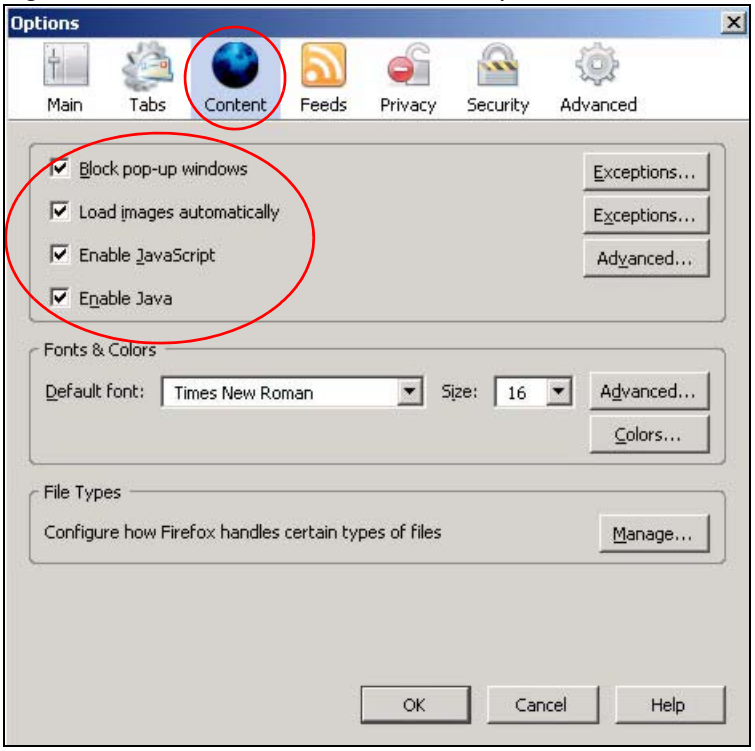
You can enable Java, Javascript and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 53 Mozilla Firefox: TOOLS > Options



Click **Content** to show the screen below. Select the check boxes as shown in the following screen.

Figure 54 Mozilla Firefox Content Security



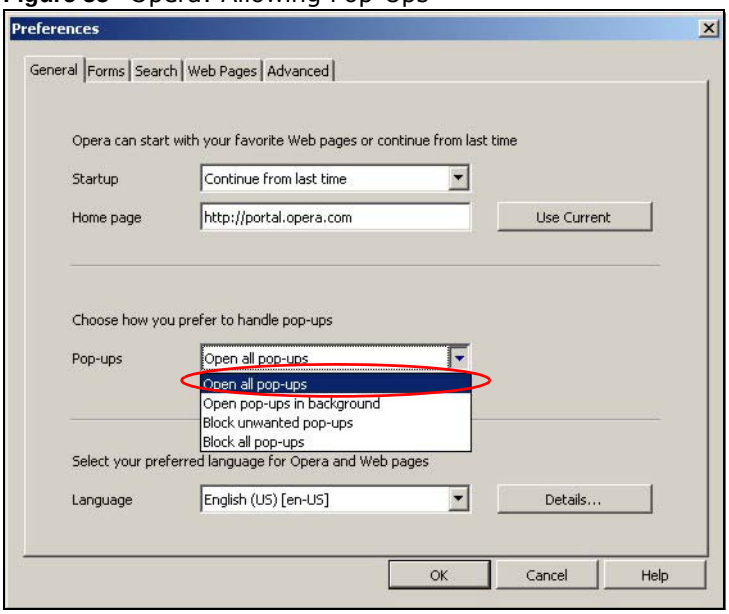
Opera

Opera 10 screens are used here. Screens for other versions may vary slightly.

Allowing Pop-Ups

From Opera, click **Tools**, then **Preferences**. In the **General** tab, go to **Choose how you prefer to handle pop-ups** and select **Open all pop-ups**.

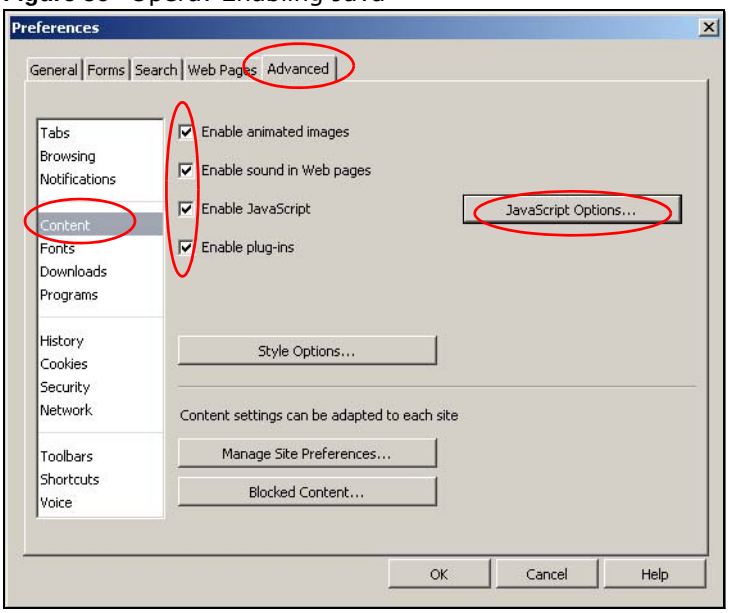
Figure 55 Opera: Allowing Pop-Ups



Enabling Java

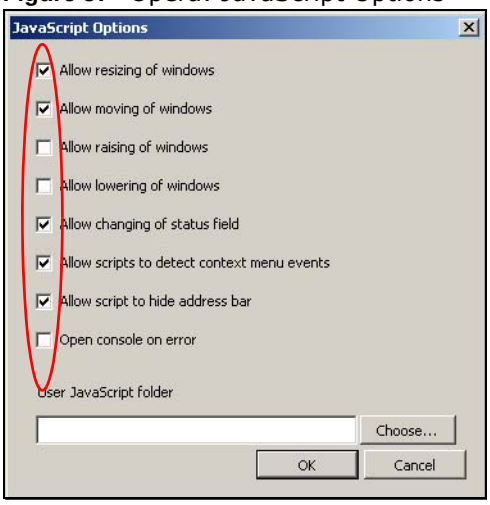
From Opera, click **Tools**, then **Preferences**. In the **Advanced** tab, select **Content** from the left-side menu. Select the check boxes as shown in the following screen.

Figure 56 Opera: Enabling Java



To customize JavaScript behavior in the Opera browser, click **JavaScript Options**.

Figure 57 Opera: JavaScript Options



Select the items you want Opera's JavaScript to apply.

C

Legal Information

Copyright

Copyright © 2013 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b, 802.11g or 802.11n (20MHz) operation of this product in the U.S.A. is firmware-limited to channels 1 through 11. IEEE 802.11n (40MHz) operation of this product in the U.S.A. is firmware-limited to channels 3 through 9.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1) this device may not cause interference and

2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IC Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

注意 ！

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

Go to http://www.zyxel.com to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Regulatory Information

European Union

The following information applies if you use the product within the European Union.

Declaration of Conformity with Regard to EU Directive 1999/5/EC (R&TTE Directive)

Compliance Information for 2.4GHz Wireless Products Relevant to the EU and Other Countries Following the EU Directive 1999/5/EC (R&TTE Directive)

[Czech]	ZyXEL tímto prohlašuje, že tento zařízení je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/EC.
[Danish]	Undertegnede ZyXEL erklærer herved, at følgende udstyr udstyr overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
[German]	Hiermit erklärt ZyXEL, dass sich das Gerät Ausstattung in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EU befindet.
[Estonian]	Käesolevaga kinnitab ZyXEL seadme seadmed vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, ZyXEL declares that this equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
[Spanish]	Por medio de la presente ZyXEL declara que el equipo cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.

[Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ ZyXEL ΔΗΛΩΝΕΙ ΟΤΙ εξοπλισμός ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕC.
[French]	Par la présente ZyXEL déclare que l'appareil équipements est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/EC.
[Italian]	Con la presente ZyXEL dichiara che questo attrezzatura è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
[Latvian]	Ar šo ZyXEL deklarē, ka iekārtas atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
[Lithuanian]	Šiuo ZyXEL deklaruoja, kad šis įranga atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
[Dutch]	Hierbij verklaart ZyXEL dat het toestel uitrusting in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EC.
[Maltese]	Hawnhekk, ZyXEL, jiddikjara li dan tagħmir jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
[Hungarian]	Alulírott, ZyXEL nyilatkozom, hogy a berendezés megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EK irányelv egyéb elõírásainak.
[Polish]	Niniejszym ZyXEL oświadcza, że sprzęt jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
[Portuguese]	ZyXEL declara que este equipamento está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/EC.
[Slovenian]	ZyXEL izjavlja, da je ta oprema v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/EC.
[Slovak]	ZyXEL týmto vyhlasuje, že zariadenia spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/EC.
[Finnish]	ZyXEL vakuuttaa täten että laitteet tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
[Swedish]	Härmed intygar ZyXEL att denna utrustning står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EC.
[Bulgarian]	С настоящото ZyXEL декларира, че това оборудване е в съответствие със съществените изисквания и другите приложими разпоредбите на Директива 1999/5/ЕС.
[Icelandic]	Hér með lýsir, ZyXEL því yfir að þessi búnaður er í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 1999/5/EC.
[Norwegian]	Erklærer herved ZyXEL at dette utstyret er I samsvar med de grunnleggende kravene og andre relevante bestemmelser I direktiv 1999/5/EF.
[Romanian]	Prin prezenta, ZyXEL declară că acest echipament este în conformitate cu cerinţele esenţiale şi alte prevederi relevante ale Directivei 1999/5/EC.

CE

National Restrictions

This product may be used in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Ce produit peut être utilisé dans tous les pays de l'UE (et dans tous les pays ayant transposés la directive 1999/5/CE) sans aucune limitation, excepté pour les pays mentionnés ci-dessous:

Questo prodotto è utilizzabile in tutte i paesi EU (ed in tutti gli altri paesi che seguono le direttive EU 1999/5/EC) senza nessuna limitazione, eccetto per i paesii menzionati di seguito:

Das Produkt kann in allen EU Staaten ohne Einschränkungen eingesetzt werden (sowie in anderen Staaten die der EU Direktive 1995/5/CE folgen) mit Außnahme der folgenden aufgeführten Staaten:

In the majority of the EU and other European countries, the 2.4-GHz bands have been made available for the use of wireless local area networks (LANs). Later in this document you will find an overview of countries inwhich additional restrictions or requirements or both are applicable.

The requirements for any country may evolve. ZyXEL recommends that you check with the local authorities for the latest status of their national regulations for the 2.4-GHz wireless LANs.

The following countries have restrictions and/or requirements in addition to those given in the table labeled "*Overview of Regulatory Requirements for Wireless LANs*":.

Overview of Regulatory Requirements for Wireless LANs			
Frequency Band (MHz)	Max Power Level (EIRP)[1] (mW)	Indoor ONLY	Indoor and Outdoor
2400-2483.5	100		V

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Please check http://www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie http://www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez http://www.ibpt.be pour de plus amples détails.

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check http://www.sviluppoeconomico.gov.it/ for more details.

Questo prodotto è conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all 'interno del proprio fondo, l'utilizzo di prodotti Wireless LAN richiede una "Autorizzazione Generale". Consultare http://www.sviluppoeconomico.gov.it/ per maggiori dettagli.

Latvia

The outdoor usage of the 2.4 GHz band requires an authorization from the Electronic Communications Office. Please check http://www.esd.lv for more details.

2.4 GHz frekvenèu joslas izmantoðanai ârpus telpâm nepiecieðama atïauja no Elektronisko sakaru direkcijas. Vairâk informâcijas: http://www.esd.lv.

Notes:

1. Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

2. The regulatory limits for maximum output power are specified in EIRP. The EIRP level (in dBm) of a device can be calculated by adding the gain of the antenna used(specified in dBi) to the output power available at the connector (specified in dBm).

List of national codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Malta	MT
Belgium	BE	Netherlands	NL
Cyprus	CY	Poland	PL
Czech Republic	CR	Portugal	PT
Denmark	DK	Slovakia	SK
Estonia	EE	Slovenia	SI
Finland	FI	Spain	ES
France	FR	Sweden	SE
Germany	DE	United Kingdom	GB
Greece	GR	Iceland	IS
Hungary	HU	Liechtenstein	LI
Ireland	IE	Norway	NO
Italy	IT	Switzerland	CH
Latvia	LV	Bulgaria	BG
Lithuania	LT	Romania	RO
Luxembourg	LU	Turkey	TR

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the power outlet.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Index

Numbers

3G 34
4G 34

A

Access Point Name 35
APN 35

C

certifications 97
  notices 98
  viewing 98
Challenge Handshake Authentication Protocol 36
Channel 23
channel 42
CHAP 36
Configuration
  restore 74
copyright 97
CPU usage 23

D

data plan 36
Daylight saving 72
DHCP 28, 51
  DHCP server
  see also Dynamic Host Configuration Protocol
DHCP server 51
disclaimer 97
documentation
  related 2
Dynamic Host Configuration Protocol 51

E

encryption 43

F

FCC interference statement 97
Firewall 64
  Firewall overview
  guidelines 64
  network security
  Stateful inspection 64
  ZyXEL device firewall 64
Firmware upload 72
  file extension
  using HTTP

G

General wireless LAN screen 43
Guide
  Quick Start 2

I

IP Address 49, 58
IP Pool 52

L

LAN 49
  IP pool setup 51
LAN overview 49
LAN setup 49
Language 75

Local Area Network 49
Long Term Evolution 34
LTE 34

M

MAC 46
MAC address 42
MAC address filter 42
MAC address filtering 46
MAC filter 46
managing the device
  good habits 11
  using the web configurator. See web configurator.
  using the WPS. See WPS.
Media access control 46
Memory usage 23
mobile data usage control 36
mobile network type 35
mobile telecommunications technologies 34
monthly limit 37

N

NAT 55, 57
  global 56
  inside 56
  local 56
  outside 56
  overview 55
  port forwarding 60
  see also Network Address Translation
  server 56
  server sets 60
Navigation Panel 23
navigation panel 23
Network Address Translation 55, 57

O

other documentation 2

P

PAP 36
Password Authentication Protocol 36
Personal Identification Number 38
Personal Unblocking Key 39
PIN 38
PIN change 39
PIN code 38
PIN remaining authentication times 38
PIN setting 37
Pool Size 52
Port forwarding 58, 60
  default server 57, 60
  example 60
  local server 58
  port numbers
  services
product registration 98
PUK 39
PUK code 38

Q

Quick Start Guide 2

R

registration
  product 98
related documentation 2
Reset button 12
Reset the device 12
Restore configuration 74
roaming 35

S

Service and port numbers 67
Service Set 44
Service Set IDentification 44

Service Set IDentity. See SSID.
Short Message Service 31
SIM card blocked 38
SMS 31
SMS box full 31
SSID 23, 42, 44
Status 20
status screen 20
Subnet Mask 50
Summary
  DHCP table 28
  Packet statistics 29
  Wireless station status 30
System General Setup 69
System restart 75

T

TCP/IP configuration 51
Third Generation 34
Time setting 71
trademarks 97

W

WAN (Wide Area Network) 33
warranty 98
  note 98
Web Configurator
  how to access 17
  Overview 17
web configurator 11
Wireless association list 30
Wireless network
  basic guidelines 42
  channel 42
  encryption 43
  example 41
  MAC address filter 42
  overview 41
  security 42
  SSID 42
Wireless security 42
  overview 42
  type 42
wireless WAN 33
WLAN 33
WLAN button 14
WPS 11
WWAN 33